Oracle Utilities Cloud Services

Administration Guide

Release 25.10
G39747-02
October 2025

Oracle Utilities Cloud Services Administration Guide, Release 25.10

G39747-02

Contents

1 Introduction

Part I Identity and Access Management with Identity Domains

2 Identity and Access Management Overview

3 Quick Start Guide

4 Security Administrator Account

5 User Management Procedures

User Onboarding 1
Advanced User and Access Management 2

6 User Provisioning for Oracle Utilities Cloud Services

User Provisioning Overview 1
Pre-Defined Application Roles 1
Configuring Just in Time Provisioning 2
Creating and Provisioning Users 4
Cloud Service Implementation User 8

7 User Provisioning for Oracle Utilities Analytic Insights

8 User Management for Oracle Utilities Analytic Insights

9 Using Federated Single Sign-On

Part II Object Storage Setup with Identity Domains

10 Object Storage Setup Overview

11 Object Storage Management

Object Storage Structure 1
Security and Access Management 2
Tenant Information 4
API Access 5

12 Connecting to Oracle Cloud Object Storage

Object Storage Connection Configuration 1
API Key Management 2
Referencing Files on Object Storage 2

13 Recommended Object Storage Structure for a New Implementation

Security Considerations 1
Recommended Setup for a Single Cloud Service 2
Recommended Setup for Multiple Cloud Services 4

14 Initial Testing of Object Storage Connectivity

15 Cross-Region Disaster Recovery Considerations

Home and Disaster Recovery (DR) Regions 1
Preparing your Disaster Recovery Region 2
Recovering from a Disaster 3

Part III Cloud Monitoring

16 Status Page

Part IV GoldenGate Replication

17 GoldenGate Replication

GoldenGate Replication Overview 1
Requirements, Prerequisites, and Assumptions 2
GoldenGate Replication Administration Tasks 3
Obtaining Tenancy Information 4
Setting Up Compartments and Security Policies 4
Setting up Virtual Cloud Networks and Subnets 7

Index

1

Introduction

Welcome the Oracle Utilities Cloud Services Administration Guide. This document provides information related to ongoing administration and maintenance of the following Oracle Utilities cloud services:

- Oracle Utilities Billing Cloud Service
- Oracle Utilities Customer Care and Billing Cloud Service
- Oracle Utilities Customer Cloud Service
- Oracle Utilities Digital Asset Cloud Service
- Oracle Utilities Market Settlements Management Cloud Service
- Oracle Utilities Meter Solution Cloud Service
- Oracle Utilities Rate Cloud Service
- Oracle Utilities Work and Asset Cloud Service

The topics described in this document include:

- Identity and Access Management with Identity Domains
- Object Storage Setup with Identity Domains
- Cloud Monitoring
- GoldenGate Replication

Part I

Identity and Access Management with Identity Domains

This section provides instructions for Security Administrators regarding how to set up user accounts for Oracle Utilities cloud services, manage the user identity lifecycle, and govern authentication in multiple business applications. Identity and access management tasks include creation of users and groups, granting access to business applications, and configuring various settings. This section includes:

- Identity and Access Management Overview
- Quick Start Guide
- Security Administrator Account
- User Management Procedures
- User Provisioning for Oracle Utilities Cloud Services
- User Provisioning for Oracle Utilities Analytic Insights
- User Management for Oracle Utilities Analytic Insights
- Using Federated Single Sign-On

Before You Begin

The chapters in this section describes how Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) is used with Oracle Utilities cloud services.

Before you begin configuring Oracle Cloud Infrastructure Identity and Access Management for your implementation, you should review the following Oracle Cloud Infrastructure documentation:

- Oracle Cloud Infrastructure Security Guide
- Security Best Practices
- Securing IAM

We also recommend you review the following technical papers and blog articles related to IAM security:

- Best Practices for Identity and Access Management (IAM) in Oracle Cloud Infrastructure
- OCI IAM Identity Domains Best Practices
- OCI IAM Policies Best Practices

2

Identity and Access Management Overview

This chapter provides an introduction to working with Oracle Cloud Infrastructure Identity and Access Management (IAM) with Identity Domains.

Oracle Cloud Infrastructure tenancy is provisioned to customers with subscriptions to Oracle Utilities cloud services. Identity and Access Management (IAM) is a built-in part of the Oracle Cloud Infrastructure, and it governs the access to Oracle Cloud Infrastructure resources and Oracle Cloud Services. Identity domains are part of IAM and is where users and access to Oracle Cloud Services are configured and managed.

Each cloud service subscription includes at least one Identity Domain. The identity domains are managed exclusively by the customer (see Identity Domains below for more information).

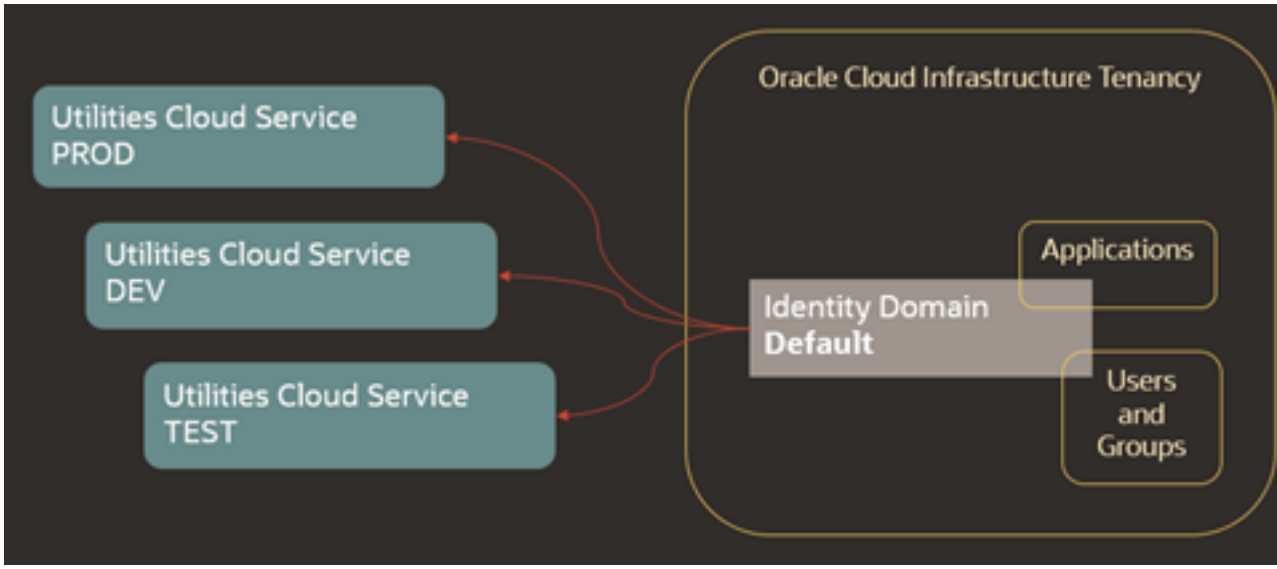
About This Section

The Identity and Access Management section of this guide contains the following:

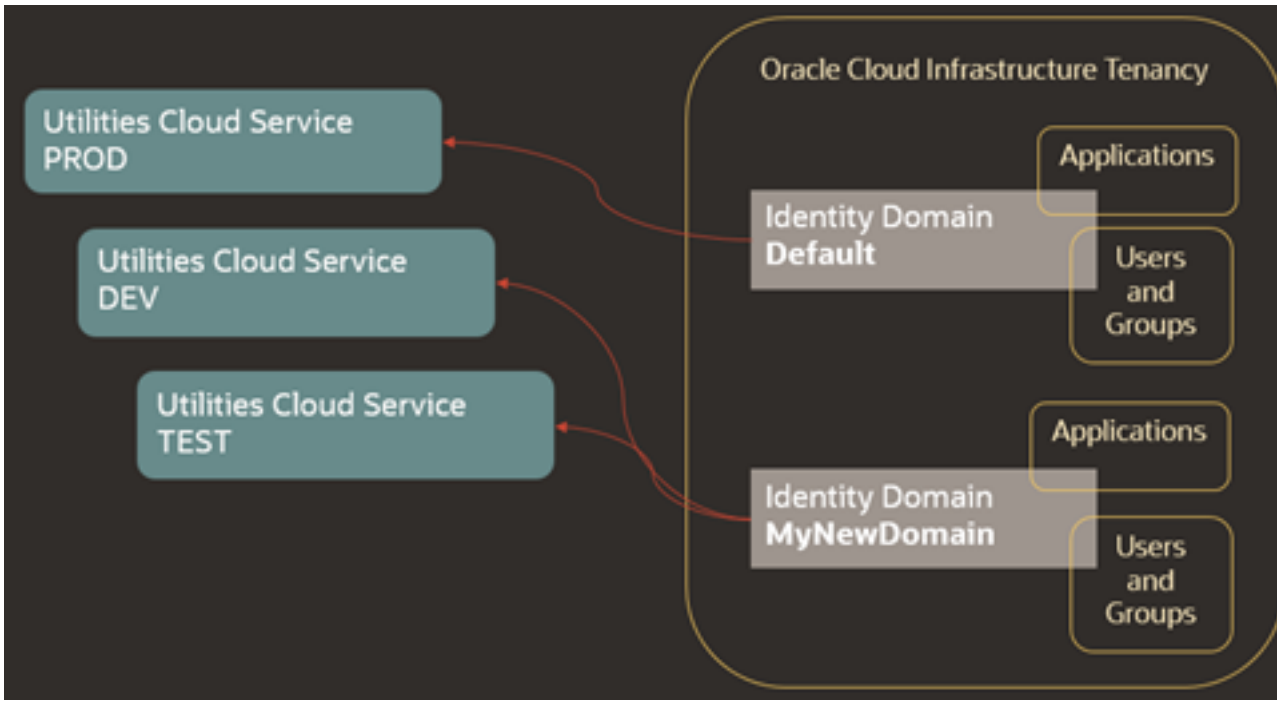
- Quick Start Guide provides an overview of the end user provisioning process, with references to additional information in the following chapters.
- Security Administrator Account describes how to set up a security administrator account for user provisioning.
- User Management Procedures describes general procedures related to managing users and groups.
- User Provisioning for Oracle Utilities Cloud Services describes specific tasks related to user provisioning for Oracle Utilities cloud services.
- User Provisioning for Oracle Utilities Analytic Insights describes specific tasks related to user provisioning for Oracle Utilities Analytic Insights.
- User Management for Oracle Utilities Analytic Insights describes specific tasks related to user management for Oracle Utilities Analytic Insights.
- Using Federated Single Sign-On describes tasks required when using an external identity management system to provide authentication for the application instances within your cloud subscription.

Identify Domains

The Oracle Utilities Cloud Service configurations are defined and maintained in an Identity Domain. Initial provision of the service results in all environments being connected to a single Identity Domain (usually a Default domain).



This topology may be modified in the future. For example, you may create an additional Identity Domain that is dedicated for production environment. In this scenario, you should submit a request for the re-connection to the Oracle support team.

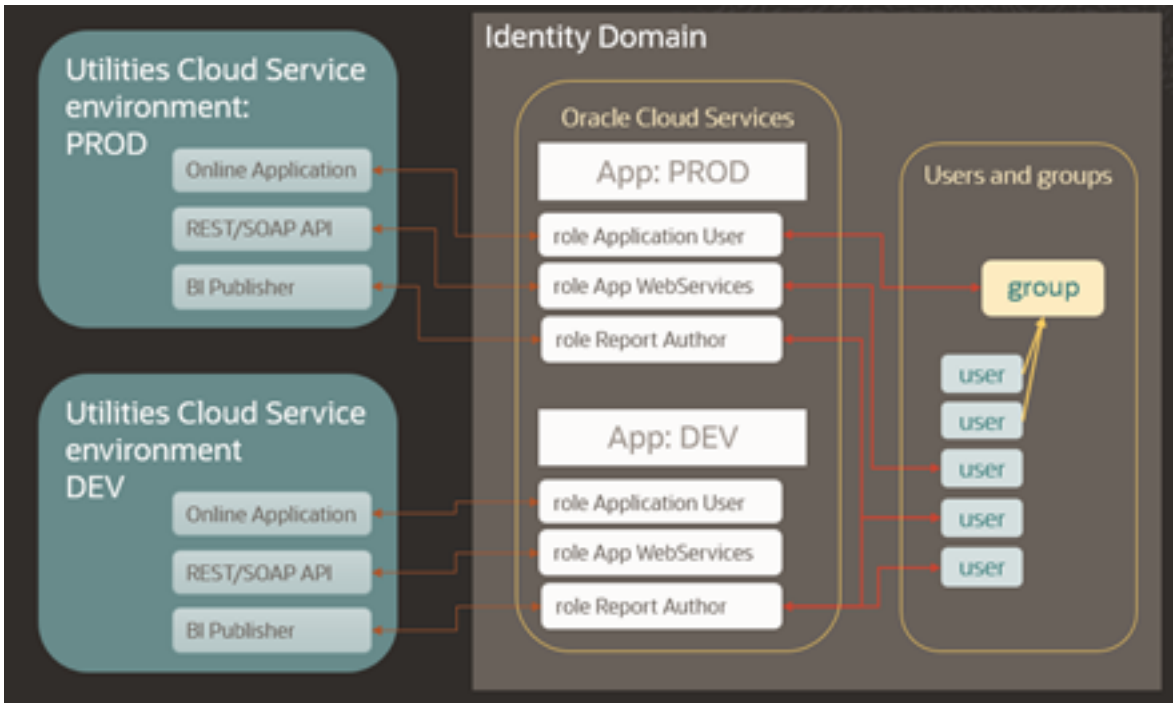


The following configurations are necessary to perform the identity and access management for the Oracle Utilities Cloud Services

- **Application**: For Oracle Utilities cloud services the application represents a single environment, Production or non-Production. Applications are created by the service provisioning process.
- **Application Role**: The Application Role represents an entitlement to access one of the components within the environment. By assigning user or groups to an Application Role

the security administrator is authorizing access to the corresponding component(s). Application Roles are created by the service provisioning process.

- **User**: Users represent a human or non-human entity that is accessing the environment. User records are created and managed by the Security Administrator.
- **Group**: Groups comprise of one or more users. Groups are created and managed by the Security Administrator.



3
Quick Start Guide

This chapter provides an overview of the initial set up of your cloud server user community including:

- Activate Security Administrator Account
- Evaluate Federated Single Sign-On Requirements
- Adjust the Default Oracle Identity Cloud Service Settings
- Prepare User Community
- Setup Process Summary

Activate Security Administrator Account

Access the Oracle Cloud Infrastructure console and perform the verification of the provisioned environments. Follow the steps described in Security Administrator Account.

Evaluate Federated Single Sign-On Requirements

If you are using Identity and Access Management (IAM) as your only identity management system, proceed with adjusting the identity domains settings and perform the user community setup.

If the user identities are managed by an existing enterprise identify management system, evaluate the Single Sign-On (SSO) requirements. If the federation is required for all user accounts, including the implementation team, immediately proceed with the federated SSO setup as described in Using Federated Single Sign-On.

Otherwise, if the federation is required for the actual production users only, it may be configured in later stages.

Adjust the Default Oracle Identity Cloud Service Settings

Locate the **Settings** menu and review and/or modify Identity Domain settings. Below are suggestions regarding some settings:

- **Domain settings**: Review the default settings; specify whether the primary email address will be also used as a user name (login)
- **Notifications**: You may want to include user names in communication emails. Update notification(s) accordingly.
  Update the notifications further to include additional details, for example the contact information of the technical support team.
- **Password Policy**: Evaluate the default Password Policy and amend according to your organization's requirements. You may return and modify it later and also create multiple policies for different groups of users.
- **Branding**: customize the look of the login page with your company's branding elements (optional).

Prepare User Community

Explore the Users list. Beside the Security Administrator account you may find a Process Automation group and user. This account is created as part of the service provisioning and is usually linked to the Security Administrator's email address. Process Automation is an internal user for inter-domain communications.

Take advantage of the user import feature to quickly establish user access to the provisioned environments, using the following steps:

- Compose initial lists of users who'll be accessing the environment(s), including:
  - Key members of the implementation team who are likely to have access to the non-production environments
  - Preliminary list of production environment users
- Define Group(s) for Just-In-Time Provisioning (if required). See **Setting Up Groups for Provisioning - Identity Domain** for more information).
- Browse the Oracle Cloud Services, locate the Application for each environment, and determine the Application Roles that users will be assigned to.
- Download the bulk upload template files and create import files for:
  - Users
  - Groups
  - Application Roles

See **Bulk Upload and Download** for more detailed information about uploading and downloading template files.

Setup Process Summary

Note that he following assumes the Security Administrator account has been activated.

- If you wish to delegate the just-in-time provisioning and access/authorization setup, assign administrator role to at least one user per environment (see Updating Security Privileges).
- Access the environment and configure Just-In-Time provisioning according to the product's specifications (see Configuring User Provisioning Rules - OUAF).
  - Setup the Identity Management Integration Master Configuration for Customer Cloud Services. Make sure the IAM Groups are the same Groups that were used for the User/Group import files.
- Perform import of Users, Groups and Application Roles using the import files prepared above (see **Bulk Upload and Download**).
- Setup at least one integration (non-human) user or OAuth client for integration per environment and communicate the credentials to the implementation team (see **Setting Up an Integration User for REST/SOAP Web Services**)
- Setup access to production environment for those users who are responsible for legacy data migration

4

Security Administrator Account

This chapter describes how to set up a security administrator account for user provisioning, including:

- Setting Up the Security Administrator Account
- Navigating to the Identity Domain
- Verifying Security Administrator Identity Domain Access
- Verifying Subscription Contents
- Exploring the Applications
- Verifying Access to Object Storage
- Verifying Security Administrator Access to Service

Setting Up the Security Administrator Account

The account for the Security Administrator is created during provisioning. The customer provides the name and the email address of the intended security administrator as part of the service order.

Once the order is completed the Security Administrator receives a user account activation email.

The activation email contains:

- Activation URL
- The user name, and may also include the temporary one-time password Click the activation link or copy the link into new browser window. Follow the

instructions on the email and the subsequent prompts to create a permanent password.

As a Security Administrator you will be prompted to enroll in Multi-Factor Authentication (also know as MFA). Choose an authentication factor that is more convenient for you and complete the enrollment.

You will be redirected to your Oracle Cloud Infrastructure console Dashboard.

> **Note**
>
> Multi-Factor Authentication is recommended for all service administrators that are accessing the Oracle Cloud Infrastructure console. A special Sign-on Policy for OCI console access is pre-seeded in the Default identity domain. After successful login you will be able to explore and adjust the sign-on policies and the MFA setup according to your implementation requirements. For more information refer to IAM MFA in the Oracle Cloud Infrastructure Documentation.

Navigating to the Identity Domain

The Identity Domain can be accessed via the Oracle Cloud Infrastructure portal.

Accessing via Oracle Cloud Infrastructure Console

On the Oracle Cloud Infrastructure console dashboard, click the hamburger menu right corner of the screen.

Find and expand the **Identity and Security** link.

Click the **Domains** option under **Identity**. You'll be redirected to **Domains** portal. When logging in for the first time, the **Domains** list will be empty. You should select a compartment from the **Compartments** list on the left navigation pane. Pick the root compartment and the **Domains** list will be reloaded.

If there is only one domain (named Default) on the list, select it. If you observe multiple domains, select the Oracle Identity Cloud Services domain.

The Domain Overview screen opens. It contains a general information such as the domain's name and description, domain type, and home region.

Note the Domain URL field. In order to retrieve detailed information about Identity Domain, compose the discovery URL by concatenating the domain URL (without port) with `/.well-known/idcs-configuration?region=true` and access it in your browser.

Verifying Security Administrator Identity Domain Access

Expand the **Security** topic on the navigation pane and click **Administrators**.

On the page, expand the **Identity Domain Administrator** section and verify that your name is on the list of Identity Domain Administrators.

Verifying Subscription Contents

Click **Oracle Cloud Services** on the navigation pane. The main panel displays a list of available applications.

The list contains Applications representing each environment in the subscription, for example Production or Test. The Application name comprise of service acronym, environment "type" and tenant identifier, for example CCS-PROD (C123456).

> **Note**
>
> A typical subscription includes one Production environment, and at least one Development and one Test environment. The number of environments depends on specific customer requirements and may include multiple Development and/or Test instances.

The list of applications may also include an instance of Oracle Cloud Object Storage.

Exploring the Applications

Click on one of the applications on the list and display the single application. Most of the information is system-generated and read-only.

Users and Groups should be assigned to Application Roles within the application in order to gain access to the environment.

Click the **Application Roles** link and review available Application Roles.

While the application represents a single environment, the different Application Roles represent different components within the environment. In order to authorize user's access to a certain

component the user has to be assigned to a corresponding Application Role. Application Roles include:

- Online Application Access
- Web services REST/SOAP API
- Access to supporting Applications such as Analytics Publisher and SQL Developer Web

Application Roles also used to support coarse-grained authorization in the target component, for example the Analytics Content Author versus an ordinary Analytics Consumer.

Verifying Access to Object Storage

Refer to Object Storage Setup with Identity Domains for more information about object storage.

Verifying Security Administrator Access to Service

As part of the service activation notifications, the security administrator is provided with URLs for all components within Production and Non-Production environments.

Perform the following steps to verify the access:

- Assign the security administrator user to both online-related and web services Application Roles in each environment (Application Role description indicates whether the access is given for online or for the REST/SOAP API).
- Access each environment via the URL for the online application; this action will provision your user into the Oracle Utilities Cloud Service application. Modify your user: add default data Access Role and Group and default To Do Role.

See Oracle Utilities Integration documentation for more details on how to verify API access.

5

User Management Procedures

This chapter general procedures related to managing users and groups, including:

- User Onboarding
- Advanced User and Access Management

User Onboarding

Users and groups are managed separately for each Identity Domain and not replicated automatically across domains. The user for the Cloud Account Security Administrator is always created by the provisioning process in the Default domain.

To onboard new users, navigate to the Identity Domain and find Users and Groups navigation links located on the left side navigation pane.

Setting Up New User

Click **Create New User** above the **Users** list.

Add User Details

Enter the minimum required information:

- Last Name
- First Name
- Email address

> **Note**
>
> By default the email address is used as the user name. Uncheck **Use Email as User Name** to enter the User Name manually.

- User Name

Optionally you can also add a User to the existing Groups. Click **Create** to complete the setup.

The new user appears on the list.

> **Note**
>
> Additional product-specific setup may be required in order to provide user authorization and Just In Time provisioning. See User Provisioning for Oracle Utilities Cloud Services and User Provisioning for Oracle Utilities Analytic Insights for more information.

Setting Up a New Security Administrator

There are multiple levels of administrative privileges that can be assigned to a new security administrator:

- Users assigned to the OCI Administrator administrative group are authorized to perform all identity and not identity-related administrative functions within Oracle Cloud Infrastructure tenancy including manage all identity domains.
  - Create a user for the new Administrator in the Default identity domain and add this user to the Administrators Group.
- Users assigned to the Domain Administrator administrative role are authorized to perform identity management-related administrative functions within a specific identity domain.
  - Create a user for the new Domain Administrator in the Identity Domain and add this user to the Domain Administrators Group
- Users assigned to the Identity Domain administrative role(s) are authorized to perform a limited set of administrative functions defined by these roles within a specific Identity Domain.
  - Create a user in the Identity Domain. Navigate to **Security**, **Administrators** and assign the user to one or more administrative roles.

Managing Groups

Click the **Groups** link on the left navigation panel to display a list of available groups.

Add New Group

To add a new group click **Create Group**.

Enter the **Group Name** and **Description** and save the new group.

Add Users

To add users to a group, click on the group name on the list or use the **Edit** menu action. The portal displays the selected group record.

Click the **Users** tab to add one or multiple users to the group.

Advanced User and Access Management

You manage applications, perform user management, and administer general and security settings also view basic reports with identity domains.

Managing Users

In addition to add and remove, the following single and multi-record actions are available on the **User** page:

- Resend Invitation
- Reset Password
- Activate/Deactivate User
- Update User information and preferences (on individual User record)
- Unlock User (on individual User record)

In addition the following actions are available:

- Import Users
- Export Users

Resend Invitation to Service

The initial email invitation to access the service is sent to the user immediately upon user record creation. This invitation is expired after certain period of time.

Reset Password

Resets a single, multiple, or all passwords. Users will receive a password reset email notification immediately

Activate/Deactivate User

User can be temporarily activated or deactivated. The email notification is sent to the user immediately.

If the deactivation lasts longer than the password rotation period the activation wil cause password reset.

Update User Information and Preferences

Updates details for individual users. In addition to the minimum required information provided during user creation the following details can be updated:

- Title
- Time Zone and Address including Country
- Preferred language
- Alternative email and contact information

Unlock User

Unlocks a locked user account. The user's account may be locked for various reasons for example after too many unsuccessful login attempts.

Select **Unlock User** from the **More** menu to unlock the locked account.

Managing Groups

Access the **Groups** portal from navigation pane. Select one or more entries from the list.

In addition to add and remove, the following actions are available:

- Import Groups
- Export Groups

Managing Applications

The applications that represent the provisioned services are pre-created during the service order processing. The Application Roles are also pre-configured.

The administrator is authorized to activate or deactivate certain applications, assign users to Application Roles and also perform import and export of application role's members.

Bulk Upload and Download

Identity and Access Management supports import and export of users, groups and application roles membership. The bulk identity data operations may be required for the fast user onboarding or as part of the federated single sign on setup.

The **Import** and **Export** actions are available on multiple pages:

- **Users** page:
  - Import all or a selected set of users
  - Export information for one or more users
- **Groups** page:
  - Import all or a selected set of groups and their member users
  - Export one or more groups and their member users
- **Application > Application Roles** page:
  - Import all or a selected set of application role's membership (users and groups)
  - Export one or more application role's membership (users and groups)

Importing

1. Navigate to the **Users**, **Groups**, or **Applications** (**Application Roles** link) page as appropriate.
2. Click **Import** on the top actions bar.
3. Download the sample file.
4. Review the sample file. Note that you can provide different type of information:
   - Users
   - Groups
   - Application Roles Membership
5. Populate the file with user's data and save.
6. Import the file into **Identity Domain**.

Exporting

1. Navigate to the **Users**, **Groups**, or **Applications** (**Application Roles** link) page as appropriate.
2. Select entries for the export.
3. Click **Export** on the top actions bar
   A notification email is sent as soon as the export job is completed and the file is available for the download.

Updating Settings

Use the navigation bar to expand the **Settings** topic. The following settings can be modified:

- **Default Settings**: Used to manage default time zone, language and audit setup
- **Session Settings**: Used to manage session expiration
- **Password Policy**: Used to amend the default password policy according to your requirements or create new password policies applicable for certain groups of users
- **Notifications**: Used to modify the default email notification templates provided with IAM and also enable or disable one or more notifications.

Notification Update Example: Welcome Email

The email notification templates are provided for multiple identity management-related events. The default content of these notifications can be amended to reflect customer's business requirements.

For example, there are two approaches to user account creation: using email address as a user name as opposed to using a manually defined user name. The former means the user knows what to specify on the login screen (email address). The later means the user name that is created manually by the security administrator has to be communicated to the user. In order to communicate the **user name** in the **Welcome** email perform the following steps:

- Select **Notification** on the left-side navigation pane.
- Click on the **Email Templates** tab
- Expand the **Welcome** template:
  In the email body the greeting line reads: Hello ${user.displayName}
- Modify the greeting to include the user name (login) as follows:
  Hello ${user.displayName} (${user.userName})

Note that other substitution variables are also available for use in the notifications. To explore the variables available to a specific template click the **Email Variables** link above the email body editor.

Updating Security Privileges

Use side navigation panel to expand the **Security** topic. Use **Administrators** link to add or remove administrative privileges from the users.

Sign-On Policies for Online Access

Identity and Access Management supports the ability to restrict web-browser-based access to the applications based on set of conditions including the user's client IP addresses. Both IP "blocklist" and "allowlist" approaches are supported.

- A blocklist defines a set of IP addresses that are blocked from the access. This approach should be used when the "bad" IP-s are well-known and permanent and the list is not expected to change very often.
- An allowlist defines the set of IP addresses that are permitted to access the application while everybody else is denied access.

In addition to IP addresses the following can be allowed or blocked:

- Specific users
- Groups
- User's administrative role in IAM
- User being authenticated by a specific external identity provider(s)

> **Note**
>
> Sign-On Policies are applied ONLY when user attempts to authenticate to IAM using a web browser. They are not applicable for requests submitted via REST/SOAP API.

Setup a Network Perimeter

A Network Perimeter represents a set of IP addresses, and can be defined as:

- A list of one or more IP addresses
- A range of IP addresses
- One or more IP addresses in IPv4 CIDR notation, which encompass all IP addresses belonging to a subnet. You can also use the IPv4 CIDR notation to refer to the entire internet: 0.0.0.0/0.

Create Network Perimeters:

- Use side navigation panel to expand the Security Topic
- Locate Network Perimeters
- Add one or more Network Perimeters that define "blocklist" and/or "allowlist" IP addresses

Setup Sign-On Policies

Sign-on policies define the set of rules used for granting the access to the applications. The out-of-box default policy contains a single default rule that grants the access to every authenticated user. You can either modify the default policy or create a new one(s).

Sign-on policy rule definition includes multiple optional conditions to filter the users and an action to **allow** or **deny** the access:

- By authenticating the Identity Provider: Denying/allowing access for users authenticated by specific external IP in case of a federated SSO
- By group membership: Denying/allowing access for specific set of groups
- By being or not being an Identity Domain administrator
- By being one of the explicit list of users
- By the user client's IP address being in one or more of the Network Perimeters

The rules on the policy are evaluated top-to-bottom. The first result halts the evaluation. Meaning if the user satisfies the rule's condition, the rule's action (**allow** or **deny** access) is applied and evaluation ends.

> **Note**
>
> The default rule on the default policy cannot be deleted, therefore it has to be modified first.

Example:

Let's assume that the requirement is to:

- Allow access from IP addresses on the company's intranet
- In addition, allow certain administrators to connect from their personal home computers
- Block anyone else

To configure this example:

- Create two new Network Perimeters:
  - **NP1-Company** to represent the intranet: specify the an entire subnet using CIDR notation, like, for example, 10.10.0.1/24, which means all addresses in 10.10.0 subnet
  - **NP2-Admins**: specify one or more IP addresses, comma-separated
- Configure Default Sign-On Policy:

- Modify Default Rule:
  - Set the rule's "*and the user's client IP address is*" condition to "*in one or more of these network perimeters*" and specify **NP1-Company**
  - Set the rule's action to "**Allowed**"
- Add new Rule:
  - Set the rule's "*And is an administrator*" condition to "true"
  - Set the rule's "*and the user's client IP address is*" condition to "*in one or more of these network perimeters*" and specify **NP2-Admins**
  - Set the rule's action to "**Allowed**"
- Add new Rule
  - Set the rule's "*and the user's client IP address is*" condition to "*Anywhere*"
  - Set the rule's action to "**Denied**"

Sample Sign-in Scenarios:

Scenario 1: An employee is trying to login from the office computer that is connected to the intranet.

- The first rule (the default rule) is evaluated first. The user's IP satisfies the condition by being on the NP1-Company perimeter. The rule's action ("*Allowed*") is applied and the user is allowed to sign in.

Scenario 2: The administrator is trying to login with admin's user name from a personal computer whose IP is listed in NP2-Admins perimeter.

- The first rule (the default rule) is evaluated first. The user's IP does not satisfy the condition by being on the NP1-Company perimeter
- The second rule is evaluated. The user's IP does satisfies both conditions: being and administrator and being on the Np2-Admins perimeter.
- The rule's action ("*Allowed*") is applied and the user is allowed to sign in

Scenario 3: The employee is trying to connect from the home computer.

- The first rule (the default rule) is evaluated first. The user's IP does not satisfy the condition by being on the NP1-Company perimeter.
- The second rule is evaluated. The user's IP does not satisfy any of the conditions: being neither an administrator nor being on the Np2-Admins perimeter.
- The third rule is evaluated. The user's IP satisfies the "Anywhere" condition.
- The rule's action ("*Denied*") is applied and the sign in is blocked. The IAM login error message: "Sign-on policy denies access." is displayed

Refer to IAM documentation for the detailed instructions regarding Sign-On Policy and Network Perimeter setup.

Available Reports

The following reports are available for review and download:

- Successful Login Attempts
- Unsuccessful Login Attempts
- Application Access
- Granted and Revoked Application Roles

6

User Provisioning for Oracle Utilities Cloud Services

This chapter describes user provisioning for Oracle Utilities cloud services, including:

- User Provisioning Overview
- Pre-Defined Application Roles
- Configuring Just in Time Provisioning
- Creating and Provisioning Users
- Cloud Service Implementation User

The information in this chapter applies to the following cloud services:

- Oracle Utilities Billing Cloud Service
- Oracle Utilities Customer Care and Billing Cloud Service
- Oracle Utilities Customer Cloud Service
- Oracle Utilities Digital Asset Cloud Service
- Oracle Utilities Market Settlements Management Cloud Service
- Oracle Utilities Meter Solution Cloud Service
- Oracle Utilities Rate Cloud Service
- Oracle Utilities Work and Asset Cloud Service

User Provisioning Overview

Each Oracle Utilities cloud service environment included in the subscription contains multiple components:

- Business Applications that run on the Oracle Utilities Application Framework, (OUAF) Oracle Utilities Application Framework supports fine-grained authorization to access various features within the Business Application. It stores users and user groups.

  For each user authorized to access Oracle Utilities Application Framework the corresponding application user is created in the Oracle Utilities Application Framework.

  For the online application access, Oracle Utilities Application Framework users are created through Just in Time Provisioning flow.
- Supplemental components such as Analytics Publisher that don't maintain their own user records and support role-based authentication and authorization.

Pre-Defined Application Roles

The roles listed below are pre-defined in the applications that represent Oracle Utilities service environments. Each role represents an entitlement within the environment and grants user an access to a certain component.

New roles may be added with future releases as the Oracle Utilities Cloud Services are expanded into new functional areas.

Application Role	Authorized Access
Online Application User	Users assigned to this role may access online application.
Web Services Access	Users assigned to this role is authorized to access the REST/ SOAP APIs.
BI Consumer	Users assigned to this role may access the Analytics Publisher within the environment and view and execute pre-defined reports.
BI Content Author	Users assigned to this role may access the Analytics Publisher within the environment and author new and view/execute existing reports.
Test Administrator	Users assigned to this role may access the Utilities Testing Accelerator within the environment and perform administrative tasks as well as develop and approve other's work.
Test Approver	Users assigned to this role may access the Utilities Testing Accelerator within the environment and develop and approve Test Components and Test Flows.
Test Developer	Users assigned to this role may access the Utilities Testing Accelerator within the environment and develop Test Components and Test Flows.
SQL Developer Web Online User	Users assigned to this role may access the Database Actions online and query the database to retrieve the information from both production and conversion schema
REST Enabled SQL	Users assigned to this role may use cURL utility to invoke REST services and query the database to retrieve the information from both production and conversion schemas.
SGG Test Harness User	Users assigned to this role may access the Smart Grid Gateway Cloud Test Harness provided with Oracle Utilities Meter Solution Cloud Service and Oracle Utilities Customer Cloud Service.

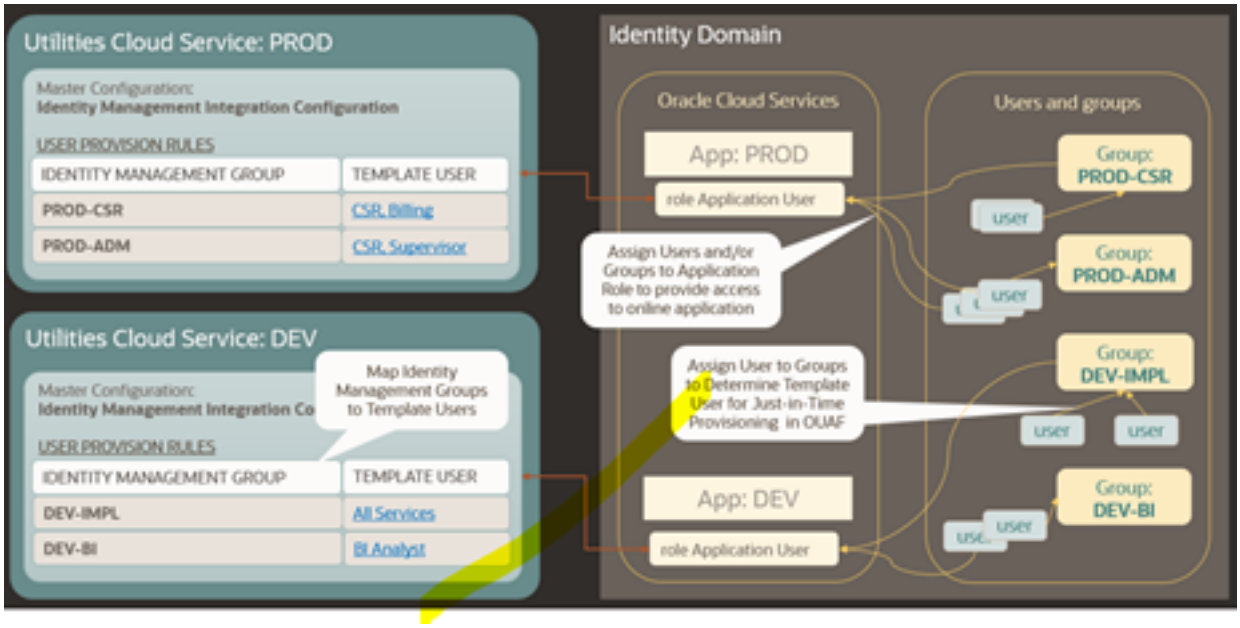
> **Note**
>
> Additional pre-defined roles for Oracle Utilities Analytics Visualization may be provided with specific cloud services. Examples include *CustomerContentCreator*. *CustomerContentConsumer* among others.

Configuring Just in Time Provisioning

Just In Time provisioning is a process that creates application user record in the OUAF- based business applications upon first successful login.

The new user is created in the business application based on a pre-defined OUAF Template User.

The Template User is determined from the mapping between Groups and OUAF Template Users defined in **Identity Management Integration Configuration**.



Steps to configure Just In Time provisioning:

- Assign Security Administrator user to a Online Application Role in the environment (this is required to access the OUAF with access administrator privileges)
- Setting Up Groups for Provisioning - Identity Domain
- Configuring User Provisioning Rules - Oracle Utilities Application Framework

Setting Up Groups for Provisioning - Identity Domain

The following is a suggested approach to Just-In-Time provisioning.

Create Groups in the Identity Domain that represent broad functional areas and/or authorization level in the service. For example:

- For Non-Production (Development and Testing) environments:
  - Implementers
  - Business Analysts
  - QA Team
  - Security Testing
  - Functional Testing
- For Production environments:
  - Call Center
  - Call Center Supervisor
  - Business Administrator
  - Accounting

Configuring User Provisioning Rules - Oracle Utilities Application Framework

To configure Identity Management Integration in the Oracle Utilities Application Framework (OUAF):

- Create Template Users that represent various level of access authorization
- Review existing Template Users.
  If your intention is to use a Template User to provision integration (non-human) users you might have to assign Default Access Group to the Template User.
- Map the Groups created above to the Template Users in OUAF in the Identity Management Integration Master Configuration.
  If the Identity Management Integration Master Configuration is not configured at the time the user record is created, the user will be provisioned with K1MINACS (default minimal access).

Creating and Provisioning Users

This section describes steps involved in creating users and providing access to the cloud service's various components.

Setting Up an OUAF Security and Access Administrator

Perform the following steps:

1. Create a new user or search for and select an existing user.
2. Assign this user to the User Administrator role. See Setting Up a New Security Administrator for more details.
3. After first login to OUAF this user will be provisioned with Template User K1SCRADM (security administrator).

Setting Up an Online Application User

Perform the following steps:

1. Create a new user or search for and select an existing user.
2. Assign the user to the group that represents the appropriate level of authorization for the environment.
3. Locate the application that is corresponding to the environment. Assign the user to the Online Application User role in the environment.

Setting Up an Integration User for REST/SOAP Web Services

REST/SOAP API doesn't perform Just-In-Time provisioning. Users for web services must be created manually in both and OUAF applications.

An email address must be provided as part of user creation:

- It is recommended that this email address is used for non-human user setup only
- All email notifications concerning user account are sent to this email address
- Security administrator must have an access to this email account

Perform the following steps:

1. Create a new user or search for and select existing user
   - Specify the email address allocated for the integration/non-human users.
   - When the activation email is received, reset the user's password and communicate the email address and password to the integration team.

2. Assign the User to the REST/SOAP Web Services role in the Application that represents the environment.
3. Login to OUAF and create a new User with Login ID = User Name. Assign the user to user groups that provide access to all or selected application services, according to the business requirements.

Notes on integration user accounts management:

- Expiring passwords may cause integration flows to stop working. Reset passwords regularly to avoid eventual outages.
- You may choose to maintain two user accounts for each integration - a "main" account and an "alternate" account - to allow a graceful switch to a new password. When required, first reset password for the "alternate" user while the "main" user is still valid and working; then reconfigure the integration to use "alternate" user credentials and only then reset the "main" account password.
- Oracle recommends that you setup a dedicated integration user account for each production and non-production environment.

Setting Up an Integration OAuth Client for REST/SOAP Web Services

External systems can securely interact with Oracle Utilities Cloud Service REST APIs using OAuth client. To set this up, follow the steps below to register and configure a new OAuth client in your Identity Domain.

Use the following procedure to create a new OAuth Client:

1. Access the Identity Domain Console
   a. Navigate to your Identity Domain and open Integrated Applications.
   b. Click **Add Application**.
2. Register a Confidential Application
   a. Select **Confidential Application** when prompted.
   b. Provide a meaningful **Name** and **Description** for easy identification.
   c. Click **Next**.
3. Configure OAuth Settings
   a. On the **Configure OAuth** screen, enable Configure this application as a client now.
   b. Choose the OAuth flow required for your integration and select the supported grant types:
      - client_credentials
      - JWT assertion
      - authorization_code (you may specify a custom redirect URI)
4. Client Type and Certificate
   a. Choose the appropriate **Client Type**: trusted or confidential
   b. Upload the client certificate, if required by your integration setup
5. Configure Token Issuance Policy
   a. Specify how tokens are issued and managed
   b. Click **Add Scopes** and select applicable scopes from the resource server application
      - Scopes may allow access to: REST APIs SOAP APIs and ORDS REST APIs

6. Finalize and Activate
    a. Review the configuration
    b. Click **Activate** to complete setup.

Once the client has been created, locate the newly created OAuth Client in the Identity Domain, under **Integrated Application**.

- The client ID and secret can be found in the **General Information** section of the **OAuth Configuration** section.
- The allowed scope can be found in the **OAuth Client** section on the **Configuration** section, under **Token Issuance Policy**.

If your integration implements Client Credentials OAuth flows, the next step is to create an application user in the appropriate Oracle Utilities Cloud Service (such as Oracle Utilities Meter Solution Cloud Service). Access the appropriate Oracle Utilities Cloud Service application, and navigate to the **User** portal.

Create a new user corresponding to the OAuth Client created above:

- Enter the OAuth client ID as the user's **Login ID**.
- Assign **User Group**(s) that will provide the integration with access to the appropriate functionality.

The OAuth Client credentials are now ready to use. When issuing a webservice call, specify the client id, secret and allowed scope that you've determined from the Identity Domain.

Maintaining OAuth Clients Created for Integration

If you created the OAuth client online, you may delete, deactivate, or regenerate the client secret as needed.

If the OAuth client was created via service request and it appears under Oracle Cloud Services, it was likely created by Oracle Utilities Cloud Operations. In that case:

- You must open a Service Request to delete, deactivate, or rotate the secret
- Provide the OAuth Client ID and Identity Domain URL

Refer to the *Oracle Utilities Cloud Services Cloud Operations Guide* for instructions.

Setting Up a User with Access to Analytics Publisher and Analytics Visualization

Perform the following steps:

1. Create a new user or search for and select an existing user.
2. Locate the application that is corresponding to the environment. Assign the user to one of the Application Roles available in the environment:
    - **Analytics Publisher**: Choose one (or both) of the following application roles:
        - BI Consumer
        - BI Content Author
    - **Analytics Visualization**: Choose one or more product-specific application roles related to Oracle Utilities Analytics Visualization features, such as CustomerContentCreator or CustomerContentConsumer. The xxContentCreator role includes access to the BI Consumer and BI Content Author roles in Analytics Publisher listed above. Similarly, the xxContentConsumer role includes access to the BI Consumer role. See Set Up a User in the *Oracle Utilities Analytics Visualization User*

Guide for more information about application roles used with Oracle Utilities Analytics Visualization.

Setting Up a User with Access to Utilities Testing Accelerator

Perform the following steps:

1. Create a new user or search for and select an existing user.
2. Locate the application that is corresponding to the environment. Assign the user to one of the Utilities Testing Accelerator roles available in the environment:
   - Test Administrator
   - Test Approver
   - Test Developer

The Utilities Testing Accelerator user must be authorized to access the Utilities Cloud Service to perform the API and online application testing.

- Assign the user to the **Online Application User** and **Web Services Access** roles.
- Request the user to login to the online application to trigger the Just -In-Time provision. This action will create user record in the Utilities Cloud Service.

Setting Up a User Authorized to Execute Ad-hoc SQL Queries

Perform the following steps:

1. Create a new user or search for and select an existing user.
2. Locate the application that is corresponding to the environment. Assign the user to one of the following roles:
   - **SQL Developer Web Online User**: Provides access to the online web-based interface that enables user to execute queries
   - **Rest Enabled SQL**: Provides the ability to execute REST calls using cURL command

Setting Up an Integration OAuth Client for Ad-hoc SQL Queries

External systems may perform Ad-hoc SQL Queries via REST API using OAuth client credentials. OAuth clients are created by Oracle Utilities Cloud Operations team (refer to the Oracle Utilities Cloud Services Cloud Operations Guide for more information).

To request creation of a new OAuth Client, create a Cloud Operations service request and provide the following information:

- **Environment**(s) where the OAuth client is needed. For example, PROD, TEST01, DEV
- **Client name suffix**: Use a distinct name that may suggest the functional purpose of the integration, for example METERDATA or whatever is applicable for the particular integration's business use. If not provided, the default suffix is INTEG
- **Client description**: Provide a meaningful description of the integration point
- **Client type (trusted or confidential) and client certificate**: The integration requirements may call for trusted client and the external application may also supply its own certificate. Otherwise, Oracle Identity Cloud Service creates trusted client with its internal native certificate.
- **OAuth flow for your intended integration**: Currently supported are client credentials, JWT assertion, and authorization code flows. For the authorization code flow you can also supply your own redirect URL.

- **Scope**: Specify that you would like to run Ad-hoc SQL query

The Oracle Utilities Cloud Operations team will create the OAuth Client using the input provided in the service request.

Once the client has been created, locate the newly created OAuth Client on the Oracle Identity Cloud Service **Admin Console**, under **Oracle Cloud Services**. The name is composed as <product>-<domain><tenant><suffix><sequential number>, for example:

```
CCS-PRODC12345CMETERDATA0 , CCS-PRODC12345FIELDSERVICE1.
```

- The client ID and secret can be found in the General section of the **Configuration Tab**.
- The allowed scope can be found in the **OAuth Client** section on the **Configuration Tab**, under **Token Issuance Policy**.

The OAuth Client is now ready to use. When issuing a RETS call, specify the client id, secret and allowed scope that you've determined from the Oracle Identity Cloud Service **Admin Console**.

> **Note**
>
> If you are planning to utilize JWT Assertion OAuth flow and authorize on behalf of a user, make sure that the user that will be performing the call is assigned to both **SQL Developer Web Online User** and **Rest Enabled SQL** application roles.

Maintaining OAuth Clients Created for Integration

You can delete the OAuth client or regenerate the OAuth client secret by creating a service request with the Oracle Utilities Cloud Operations team. Provide the OAuth Client ID and the Oracle Identity Cloud Service tenancy URL. The Oracle Utilities Cloud Operations team will perform the requested action on your behalf. Refer to the Oracle Utilities Cloud Services Cloud Operations Guide for more information about working with the Oracle Utilities Cloud Operations team.

Setting Up a User with Access to the Smart Grid Gateway Test Harness

Perform the following steps:

1. Create a new user or search for and select an existing user.
2. Locate the application that is corresponding to the environment. Assign the user to following role available in the environment:
   - SGG Test Harness User (SGGHarnessUser)

Cloud Service Implementation User

The environment provisioning process creates an internal (non-human) user account named "K1IPROCESS" that is used by cloud service implementation tools and processes, including configuration migration between environments.

7

User Provisioning for Oracle Utilities Analytic Insights

This chapter describes user provisioning for Oracle Utilities Analytic Insights, and includes the following:

- Overview
- Pre-Defined Application Users
- Setting Up Application Users

Overview

Oracle Utilities Analytic Insights features internal user access management that grants users the access to various features within the application. It stores and maintains users.

For each user that authorized to access Oracle Utilities Analytic Insights the corresponding application user is created in OUAI.

The Oracle Utilities Analytic Insights user is created thru Just in Time Provisioning flow.

Pre-Defined Application Users

The following roles are pre-defined in the Applications that represent Oracle Utilities Analytic Insights environments:

Application Role	Authorized Access
Online Application User	The user assigned to this role may access online application
Online Application Admin	The user assigned to this role may access the online application and also perform the administrative tasks in Oracle Utility Analytic Insights.
BI User	The user assigned to this role may access the Oracle Business Intelligence Enterprise Edition (OBIEE) component within the environment

In addition to the above listed roles, BIConsumer, BIContentCreator, and Analytics Visualization roles may also be provisioned.

Setting Up Application Users

Perform the following steps to provision new user:

1. Create a new user or search for and select an existing User.
2. Locate the application that is corresponding to the Oracle Utilities Analytic Insights environment.
3. Assign the user to one of the Online Application roles.
4. Assign the user to the BI User role

8

User Management for Oracle Utilities Analytic Insights

Once the user has been created and assigned to the application role(s), the user may access Oracle Utilities Analytic Insights online.

Upon first successful login, the user record is created in the Oracle Utilities Analytic Insights user list, and is ready to be configured and assigned to Oracle Utilities Analytic Insights groups and roles. Groups and roles determine the user features and functionality available to each user.

This chapter outlines specific steps that need to be performed to configured users in Oracle Utility Analytic Insights including:

- Locating Provisioned Users in Oracle Utility Analytics Insights
- Assigning Groups and Roles in Oracle Utility Analytic Insights
- Assigning and Removing User Group Permissions

Locating Provisioned Users in Oracle Utility Analytics Insights

Once a user has been created in Identity and Access Management and logged into the application for the first time, it will appear in the Oracle Utility Analytic Insights user list. See User Management for Oracle Utilities Analytic Insights

> **Note**
>
> You need to have customer administration rights to complete this task. Verify that your user has been assigned to the Application Admin role in the application that is corresponding to the environment.

Use the following procedure to locate a user.

1. Log in to Oracle Utility Analytic Insights.
2. Select **Administer**, then **Security**, then **Users** to navigate to the **Administer Users** page.
3. Search for the user you created in IAM by completing one of the user information fields and then clicking **Get Users**.
   You may search for a user by any data entered when creating the user.

   The data table will return with the user information and links that allow you to assign their user environment. See the Oracle Utilities Analytic Insights documentation for additional information about the **Administer User** page.
4. Click **Edit** in the user row to open the **Manage Users** dialog box. The **Manage Users** dialog box allows you to modify group and role permissions.

Assigning Groups and Roles in Oracle Utility Analytic Insights

User environment access is managed through the Add Group and Add Role functions located in the **Mange Users** pane.

- **Add Group**: Determines general user interface characteristics (for example, the menus that are displayed) and, consequently, which pages are accessible to the user and sets of users.
- **Add Role**: Assigns user roles and determines the features that are available on the pages made available by the user's group privileges.

Roles are associated with modules. Assigning a role automatically associates the user to a module. The following table provides an example of possible user role to module associations. See the Oracle Utilities Analytic Insights documentation for more information.

Module	Role
Meter to Bill	AMI Deployment Billing Meter Operations Safety
Revenue Protection	Revenue Protection
Distribution Planning and Operations	Distribution Planning
Demand Response and Energy Efficiency	Demand Response and Energy Efficiency

Most end users have access to environments with Explore and Export functionality based on their group assignment. The features available for the user on the Explore and Export pages are determined by their role. For example, a user with a Billing role in the Meter to Bill module has different algorithms and panels on the Explore page than a user assigned to the Distribution Planning role in the Distribution Planning and Operations module.

> **Note**
>
> The user interface features defined for groups and roles are determined by licensing and implementation. They are not configurable by the customer.

Assigning and Removing User Group Permissions

The **Group** options in this section are examples only. Your environment may have different group types or group names.

Assigning User Group Permissions

Use the following procedure to assign a user to a group:

1. Locate the user in Oracle Utility Analytic Insights and open the dialog box for the user. See Locating Provisioned Users in Oracle Utility Analytics Insights.
2. Click **Assign Additional Group**.
3. Select the appropriate group from the **Add Group** drop-down list, and click **Save**. The **Manage Users** dialog box will update the **Group** field with the assigned group.
4. If a user needs permissions for multiple groups, repeat the previous steps for each additional group.
5. Click **Cancel** or any area outside of the dialog box to close the dialog box.

Removing User Group Permissions

Use the following procedure to remove group assignments:

1. Open the **Manage User** dialog box for the user. See Locating Provisioned Users in Oracle Utility Analytics Insights.
2. Click **Remove** next to the group name you want to remove.

Assigning User Role Permissions

Users must be assigned roles in order to access the environment. Once assigned roles, a user will be able to choose from the modules that correspond to their assigned roles.

Use the following procedure to assign user role permissions:

1. Open the **Manage User** dialog box for the user. See Locating Provisioned Users in Oracle Utility Analytics Insights.
2. Click **Assign Additional Role**. The dialog will update with a drop-down list of the available roles based on the modules licensed to the customer.
3. Select the appropriate role from the list and click **Save**. The **Manage Users** dialog box will update the **Role** field with the newly assigned role.
4. If the user needs permissions for multiple roles, repeat the steps for each additional role.
5. Click **Cancel** or any area outside of the dialog box to close the dialog box.

Removing User Role Permissions

Use the following procedure to remove user role permissions:

1. Open the **Manage User** dialog box for the user. See Locating Provisioned Users in Oracle Utility Analytics Insights.
2. Click **Remove** next to the role.

9

Using Federated Single Sign-On

This chapter describes tasks required when using an external identity management system to provide authentication for the application instances within your cloud subscription, including:

- Overview
- Setup External Identity Provider
- Service Access for Federated Users
- Just In Time Provisioning for Federated Users

Overview

Federated Single Sign-On (SSO) allows your organization to use an external identity management system to provide online authentication for the application instances within your cloud subscription.

- The configuration and verification of the Federated Single Sign On should be available after the subscription is live.
- The Federated Single Sign-On only concerns online access; it is not applicable for the integration and other non-human accounts.
- The option to federate IAM Identity Domain with an external Identity and Access Management system is supported with as part of Oracle Utilities cloud service subscription.

Setup External Identity Provider

Configure a SAML 2.0 external identity provider such as Active Directory Federation Services (AD FS) for federated SSO with the IAM Identity Domain.

Configuration steps include:

- Setup the SAML 2.0 Identity Provider.
- Verify Federated Single Sign-On.
- Establish user synchronization between the Identity Domain and the SAML Identity Provider. It is necessary to copy users into Identity Domain because the access to the service is granted by assigning users to the Application Roles in Oracle Cloud Services.
  - Configure Microsoft Active Directory Bridge or implement user data synchronization via REST SCIM API, flat file import, or using one of the pre-defined provisioning Applications from the IAM catalog. Refer to the IAM documentation for more details.

To access detailed configuration instructions provided by IAM:

- Return to the Oracle Cloud Infrastructure console, expand the hamburger menu on the top left corner and select **Identity**. Click the **Identity** link and load the **Overview** page. Use one of the quick links to access documentation and tutorials on SAML SSO configuration. **Note on Identity Bridge setup only:** Federated authentication is enabled by default. This configuration means the user credentials will be validated against a configured Identity Provider. When configuring Identity Bridge define the federated authentication as follows:

  - To continue validate credentials and maintain passwords and password rules in the external identity management system leave the **Federated Authentication** checkbox checked
  - To validate credentials and manage passwords in IAM uncheck the **Federated Authentication** checkbox. IAM will generate the password for the users and send the notification by email (the email attribute must be filled in Microsoft Active Directory and mapped to the Identity Domain).

Service Access for Federated Users

Federated users should be granted access to the environments the same way as the users created directly in the Identity Domain.

See Setting Up an Online Application User and Setting Up Application Users for the instructions on how to assign user to the online access application roles.

Possible approaches:

- Process users one by one: locate user in Identity Cloud Service and assign to the application roles
- Process multiple users:
  - Export users from directly or from the group (see Exporting for more details).
  - Copy the information into Application Role import file and import users and/or groups to the Application Role (see Importing for more details).

Just In Time Provisioning for Federated Users

In the federated SSO scenario the Identity Cloud Service users and groups are imported from the external identity provider's data repository.

- Evaluate the groups created in the Identity Domain as a result of sync with external Identity Provider and determine whether to use them for Just In Time provisioning purpose.
- Login to the OUAF-based application and set up Template Users that represent authorization levels corresponding to the IAM groups synchronized from the external provider.
- Configure the **Group - Template User** mapping in the Identity Management Integration Master Configuration.

See Configuring Just in Time Provisioning for more detailed configuration instructions.

Part II

Object Storage Setup with Identity Domains

This section describes the required tasks for connecting your cloud service to Oracle Object Storage and the basic administration needed for implementation when using identity domains. This includes:

- Object Storage Setup Overview
- Object Storage Management
- Connecting to Oracle Cloud Object Storage
- Recommended Object Storage Structure for a New Implementation
- Initial Testing of Object Storage Connectivity
- Cross-Region Disaster Recovery Considerations

10

Object Storage Setup Overview

Oracle Cloud Object Storage is a part of Oracle Cloud Infrastructure Storage Services and it is a required service for Oracle Utilities Cloud Services, including Oracle Utilities Customer Cloud Service (CCS).

These cloud services uses Oracle Cloud Object Storage as the vehicle to exchange data files with customers during an implementation and in production.

Oracle Infrastructure Services get provisioned separately from Oracle Utilities Cloud Services but are grouped together under the same customer Cloud Account.

Access and administration of Oracle Cloud Infrastructure Services is done via the Oracle Cloud Infrastructure Console.

This document describes the tasks that are required for connecting the system to Object Storage and the basic administration that is needed for implementation stages and beyond that.

For more information on Oracle Cloud Object Storage (including concepts, security best practices, and more), please refer to the Object Storage documentation at: https://docs.oracle.com/en-us/iaas/Content/Object/home.htm.

This section provides information about setup and configuration of object storage for use with Oracle Utilities Cloud services, including:

- Object Storage Management
- Connecting to Oracle Cloud Object Storage
- Recommended Object Storage Structure for a New Implementation
- Initial Testing of Object Storage Connectivity
- Cross-Region Disaster Recovery Considerations

11

Object Storage Management

This chapter outlines the basic administration tasks of Oracle Cloud Infrastructure related to Object Storage, including:

- Object Storage Structure
- Security and Access Management
- Tenant Information
- API Access

Object Storage Structure

This section provides an overview how object storage is structured, including:

- Compartments
- Object Storage Buckets

Compartments

All cloud infrastructure resources are organized in Compartments.

A tenancy can include several compartments. A compartment is a logical grouping of resource types. For object storage, compartments help manage the structure of objects that are stored in the cloud.

Compartments can have child-compartments which support multi-level hierarchy of resource grouping.

Each compartment is identified by a unique Oracle Cloud ID (OCID).

When connecting the system to object storage, the compartment identification is part of the required connection configuration information.

There are no hard requirements as to the structure or number of compartments that should be created. A recommended setup is described later in this document and has reference to compartments as well.

Root Compartment

The Root Compartment is created for each account and is the top level of the compartment hierarchy. The name of that compartment includes the string "(root)" in it.

Object Storage Buckets

Oracle Cloud Object Storage is organized in buckets. A bucket is like a folder or a directory that stores one or more objects. Objects can be any file and can includes documents, images, and so on.

Each compartment can have one or more buckets. Buckets cannot include other buckets.

An example of Object Storage structure might be as follows:

- Root Compartment
  - Compartment A
    - Child Compartment A1
      - Bucket A1-1
      - Bucket A1-2
      - Bucket A1-3
    - Bucket A1
  - Compartment B
    - Bucket B1
    - Bucket B2

Bucket names are unique within a tenancy which means that the same bucket name cannot be used in different compartments. Compartments have a unique identifier (OCID) so they are in fact unique within the tenancy.

The system can be configured to connect to any compartment and bucket that you define. This configuration is described in the next chapter.

Virtual Folders

While the structure of buckets is flat across the tenancy, you can simulate a hierarchy within a bucket by using the "/" notation in the object name. For example, you can have the following objects "A/file1.dat" and "B/file1.dat" inside a bucket named "ABC". While bucket "ABC" will physically have 2 objects in it, it can also be represented as also having "A" and "B" virtual folders, both containing a file named "file1.dat".

Security and Access Management

Oracle Utilities Cloud Services security is managed by Oracle identity domains. Each Cloud Account has a default identity domain but can have multiple domains.

When a new Cloud Account is created, the Default identity domain is where you would typically define your security settings for managing your infrastructure services (including Object Storage). While additional identity domains can be created, this chapter will focus on activities and settings in your default domain.

Identity Domain management is done via the Oracle Cloud Infrastructure Console (OCI Console).

Accessing the Oracle Cloud Infrastructure Console

Once your cloud service has been provisioned, you should receive an email with the link to your Cloud Account. That link will take you to your Oracle Cloud Infrastructure (OCI) Console. In your OCI Console you will have access to manage your infrastructure resources as well as your users and their access to the various resources .

Managing Users

There are two types of users that should have access to infrastructure services (Object Storage being one of these): Human users and System Account users.

Human users should typically include two types of users:

- Administrator level personnel that use the OCI Console to manage security and the various infrastructure services (such as Object Storage).
- Business users that need access to various resources as part of the normal operations of the business. For example, such users may need access to create, modify and delete Objects in Object Storage but will not have access to administrative functions beyond that.

System Account users are applications that use an API to access the various services but do not have access to the OCI Console.

Human users will typically require email information as part of their registration while System Account users might not.

> **Note**
>
> Please refer to your Identity Domain settings to set whether an email is always required for new users. If an email is required, you will need to assign a special email address to the System Accounts that will be required for your cloud service connection to Object Storage.

Both Human users and System Account users should be assigned to User Groups that together with Policies define their access rights to various resources provided as part of your cloud service.

The process of creating a new user is described in previous chapters. This section focuses on users' unique attributes, groups and policies that will govern user access for both, Human and System Account users.

User Identification

A User is identified by an OCID key that is displayed underneath the user name. This is especially important for System Account users when configuring the connection from your cloud service to Object Storage. The OCID is the unique identifier of the user when making API calls to various infrastructure services, including Object Storage.

User API Keys

While any user can have registered API keys, they are required for System Account users that will be used for API access. The API key registered for a user is the public portion of an encryption key pair (private/public) in PEM format.

To register a public key for a User:

1. From the **User** list in your OCI Console, under your default **Identity Domain**, select the **User** name to go to the **User** details page.
2. Select the **API Keys** option from the **Resource List** on the left for that User.
3. Click **App Public Key**.
4. Select the **Paste Key** option to paste the public key content into the page and click **Add**.

There are other options to import a public key, including the actual generation of a key pair in OCI. The API keys that will be registered for Object Storage access from your cloud service will require the **Paste Key** option.

Managing Groups

Security management is done in Oracle Cloud Infrastructure by User Groups. Oracle Cloud Infrastructure includes an Administrator User Group that is predefined and contains the initial administrator user.

Adding a New User Group

1. In order to add a new user group, use the upper left menu in the **Infrastructure Console**, select **Identity & Security**, then **Domains** (under the **Identity** section). Make sure you select the root compartment and from the domain list select your default domain.
2. Under the **Identity Domain** section select **Groups** and click **Create Group** to create a new group.
3. Provide a **Name** and a **Description** for the group. Tags are optional and are not covered in this document.

Adding Users to a User Group

Users can be added to user groups in two ways:

1. When editing a user group record, you can add a user from the **Users** section by selecting **Users** from the resource list and clicking **Add Users to Group**.
2. When editing a user record, select the **Groups** option from the **Resource** list and click **Assign Users to Group**.

Managing Policies

Policies can be used to enforce access rights for Users that are a part of a User Group. Similarly to Compartments, Policies are managed at your tenancy level and not at the Identity Domain level (for example for Users and Groups).

Policies are defined using the **Identity**, **Policies** menu.

Using policy definitions, you can define the access rights to your infrastructure services, for example, Object Storage. You can define what compartment or bucket user groups have access to, and the type of access (read, write, and so on).

Policies can apply to specific compartments or the root compartment, in which case it will apply to all of the compartments. A policy is a collection of statements with specific syntax that describe access rights to resources. For example, in a policy, you can define that a certain user group has access to create and delete buckets and objects in a certain compartment.

Refer to Oracle Cloud Infrastructure documentation for Identify and Access Management with Identity Domains to find out more about policies.

Tenant Information

Information about the tenancy is displayed when selecting **Governance & Administration** from the left side menu in your OCI Console and then selecting **Tenancy Details** under the **Account Management** section.

The information displayed is important for connecting the system to Object Storage, and includes:

- The OCID key of the tenancy: This is the tenancy identification.
- Home Region: This is the main data region selected for this tenancy. Additional data regions added to this tenancy can be defined.

- Object Storage Namespace: This identifier is pre-generated and is needed for the connection of the system to Object Storage.

Regions

When a cloud account is created, a Home Region is assigned to it. This will be the Home Region you selected when you activated your order and created the account. The Home Region is the main data region that is linked to that account. Additional data regions can be subscribed to for the tenancy if access to regions outside the home regions are required.

The list of all available regions is displayed by selecting **Region Management** under the **Account Management** section of the **Governance & Administration** page. Clicking **Subscription** for a region will add that to the list of available regions for this tenancy. All administration tasks will be conducted at the home region but will be synced to the other regions automatically. Please note that when connecting the system to object storage the region has to be identified as well.

API Access

Oracle Cloud Object Storage can be accessed via the **Infrastructure Console** or via three types of APIs:

- Command Line Interface (CLI)
- REST calls
- Java SDK

The system connects to Object Storage using REST calls to the Object Storage endpoints that are documented for each of the data regions to which your cloud service has access.

For more information about Object Storage APIs, please refer to Oracle Cloud Infrastructure Object Storage documentation.

12

Connecting to Oracle Cloud Object Storage

The system supports and manages connections to Object Storage via metadata configuration. The system can connect to any number of Object Storage locations and Tenancies.

REST API calls issued by the system, to interact with the Cloud Object Storage, require an API key signature. The system is designed to have a unique private/public key pair for each environment that connects to Object Storage. This means that each system environment should have a unique System Account user defined in your default Identity Domain with a registered unique API Key.

Currently the system supports accessing files on Object Storage via batch processing. Referencing a file location as Object Storage is done using a special notation.

This chapter includes the following:

- Object Storage Connection Configuration
- API Key Management
- Referencing Files on Object Storage

For additional information refer to **External File Storage** help topic in the cloud service online help.

Object Storage Connection Configuration

Each connection configuration is represented in the system via the File Storage Configuration extendable lookup (F1-FileStorage). Each value for that extendable lookup should contain the information described below.

In order to configure a new connection, go to the Extendable Lookup portal by selecting **Admin**, then **General**, then **Extendable Lookup**, then **Search**, and search for "File Storage Configuration". After selecting it, click **Add** to add a new value.

When adding a new value, select the Oracle Cloud Object Storage file adapter and provide the following information:

- **User**: the System Account user identification (OCID Key) that is used for that connection. A unique System Account user ID should be defined for each system environment (for example Dev, Test, Prod) that is connecting to that object storage tenancy. This System Account user should not be used for other purposes.

  If one system environment is required to connect to multiple object storage tenancies, there should be a different System Account user ID for each of these tenancies.
- **Tenancy**: the tenancy ID (OCID Key) of the object storage tenancy.
- **Compartment**: the compartment ID (OCID Key) of the compartment for that connection. Each compartment can have a separate connection configuration but this is not mandatory. In fact, the compartment ID is optional for many Object Storage operations.

  However, it is recommended that you provide a compartment ID value in that field for future supported operations that might require a reference compartment, and as a good self documenting configuration practice.

You can provide the value of a parent compartment for a connection to Object Storage buckets within that compartment or all of its sub-compartments. For example: if you have a compartment "A" with 2 sub-compartments. "AB" and "AC" and you have the same security access requirements for buckets in compartment "A", "AB" and "AC" you can specify the OCID of compartment "A" in your connection configuration details instead of creating separate connection configurations for "AB" and "AC".

- **Namespace**: the Namespace of the object storage tenancy.
- **Key Ring**: the Key Ring name that was created in the system. See API Key Management for more information.
- **Region**: the region of the object storage tenancy for that connection. Reminder: object storage tenancies can have multiple regions if additional subscription was done.
- **Bucket Name Prefix**: a name prefix that will be added to the bucket name of file paths referencing object storage (see Referencing Files on Object Storage for more information).

API Key Management

Secured access to Object Storage is accomplished by using API Signature Key. Each configured connection to Object Storage includes a Key Ring.

A key ring is an object that hold a set of private/public encryption key pairs. Object Storage connections can share the same key ring and even the same key in the key ring for the same system environment.

For example, key ring A can be defined and used in all the system environments: Dev, Test, and Prod. However, the key pairs inside the ring have to be different in each of the environments. The connections defined for Object Storage can all use the same key ring A in all the environments since the actual key pair that is used in each environment, is different.

To create a new key ring, select **Admin**, then **Security**, then **Add Key Ring**. Make sure to generate a key pair in that ring after creating it.

Registering the API Key

Once a key ring has been created with an active key pair, click **View** for the Public Key of that key pair to copy the public key content. That content should be pasted into the System Account user API Key in your default Identity Domain (see the User API Keys section in Security and Access Management of Object Storage Management).

Referencing Files on Object Storage

Reference to Object Storage can be used anywhere that a file location reference is allowed in the system.

The format is file-storage://<File Location>/<Bucket>/<Filename.ext>,

where:

- **<File-Location>**: The File Storage Configuration extendable lookup value defined for that file. This will include the compartment identification.
- **<Bucket>**: The object storage bucket in the compartment that is defined as part of the File Storage Configuration extendable lookup value.
- **<Filename.ext>**: The name of the file.

For example, the "payment_info.dat" file in the "Payment-Upload" bucket in a compartment that is referenced in the "AB-Payments" File Storage Configuration extendable lookup value can be referenced as "file-storage://AB-Payments/ Payment-Upload/payment_info.dat".

Using the Bucket Name Prefix

If you set the Bucket Name Prefix in the File Storage configuration, any file path referencing this configuration will be automatically revised at runtime, adding the name prefix to the bucket name.

This allows you to define different name prefix for buckets for each environment (or for production vs non-production environments) and keep your file paths for your batch jobs the same in each environment.

For example:

- You can create all your non-production buckets with a "NP-" name prefix, and all your production buckets without a name prefix.
- You can then define a File Storage configuration named "OS-APP" in each of your environments and set the **Bucket Name Prefix** to:
  - "NP-" in all of the non-production environments
  - Blank in the production environment
- When you will use a file path reference on your batch jobs, for example "file- storage://OS-APP/AB-Payments" then:
  - When the job related to that file runs in a non-production environment it will reference the payment files in the "NP-AB-Payments" bucket.
  - When the job runs in the production environment it will reference the "AB- Payments" bucket.

13

Recommended Object Storage Structure for a New Implementation

This chapter describes a recommended configuration and structure for your Object Storage tenancy for your service implementation. Using the recommended setup can simply the initial implementation and testing activities of your new service but they are not mandatory. Furthermore, you can start with the recommended setup and adjust it per your implementation needs.

Refer to the following topics in the Cloud Service Foundation online help:

- Object Storage
- Process Automation Tool
- Data Conversion

This chapter includes the following:

- Security Considerations
- Recommended Setup for a Single Cloud Service
- Recommended Setup for Multiple Cloud Services

Security Considerations

The system connection to Oracle Cloud Object Storage is governed by a combination of User, User Group (optional) and Access Policies that are defined in your default Identity Domain (see the Object Storage Management chapter for more information). As a reminder, the User ID details are provided as part of the File Storage Extendable Lookup value in the system.

Compartments

It is recommended to divide your resources amongst several compartments:

- **Production Compartment**: This compartment includes all the production resources (such as object storage buckets and objects that store production data).
- **Non-Production Compartment**: This compartment includes all the non- production resources used during the implementation and testing phases.
- **Shared Compartment**: This compartment is used to hold resources that are used by special activities or processes and can be accesses by production and non-production users. A good example of that can be configuration data (that can be exported from a testing environment and moved to the production environment when ready, using the Content Migration Assistant) or conversion

data that can be used in both production and non-production environments (during the implementation phases).

Users

It recommended that each system environment uses a unique System Account user ID so that access rights to production vs non-production files or objects can be enforced for that tenancy.

Each System Account user will have its own API Key registered. Human users should be created if needed to manage the tenancy resource and to perform the daily operations needed for the system (such as uploading files into Object Storage). All users should be assigned to a user group, which will simplify the security access definitions.

User Groups

It is recommended to assign the users to several groups, for example:

- **Application Access User Group for Production**: This group includes the System Account users assigned to the production system environment. These users will access object storage via API calls.
- **User Access User Group for Production**: This group includes all the Human users that will need access to object storage production information. These users will typically access object storage via the OCI Console.
- **Application Access User Group for Non-Production**: This group includes the System Account users assigned to the non-production system environments. These users will access object storage via API calls.
- **User Access User Group for Non-Production**: This group includes all the Human users that will need access to object storage non-production information. These users will typically access object storage via the OCI Console.
- **Drop Partition Approval Request Requester User Group**: This group includes all the Requester users that will need access to drop a partition. These users will drop a partition through ILM Dashboard.
- **Drop Partition Approval Request Approver User Group**: This group includes all the Approver users that will need access to view and approve/reject request to drop a partition. These users will perform this action through ILM Dashboard.

These groups can be referenced when defining the security policies for production and non-production access.

Policies

It is recommended to create Policies to control access to resources based on:

- **Production vs Non-Production**: For example, it is recommended to restrict access to production resources only to production users.
- **System Account vs Human users**: For example, it is recommended to restrict certain operations from System Account users (such as the ability to delete buckets).

Recommended Setup for a Single Cloud Service

If you are using a single Oracle Utilities cloud service (such as Customer Cloud Service) consider the following recommended setup:

Object Cloud Infrastructure - IAM and Object Storage

Compartment and Buckets

- Root Compartment
  - CCS-Prod (Compartment)
  - CCS-Non-Prod (Compartment)
  - CCS-Shared (Compartment)

    * CMA-Files (Bucket) [for the system Content Migration Assistant]
    * CONV-Upload (Bucket) [for Data Conversion]
    * CONV-Output (Bucket) [for Data Conversion]

System Account Users and User Groups for Object Storage

- CCS-DEV (for the Development environment) [part of User Group CCS-OSNonProdApp]
- CCS-TEST (for the Testing environment) [part of User Group CCS-OSNonProdApp]
- CCS-PROD (for the production environment) [part of User Group CCS-OSProdApp]

Additional environments will each have their own unique User with the "CCS" prefix and will be a part of the CCS-OSNonProdApp User Group.

Policies for Object Storage

- Policy for System Account users access to object storage in the Production Compartment:
  - Typically defined under the root compartment.
  - Open only to production user groups.
  - Allows read access to buckets and read, create, modify and delete access to objects in the Production Compartment and the Shared Compartment.
- Policy for System Account users access to object storage in the Non-Production Compartment
  - Defined under the root compartment.
  - Open only to non-production user groups.
  - Policy details can resemble the production policy or be less restrictive in terms of access allowed for buckets.
- Policies for Human users can be similar to the policies for System Account users but can allow more access for managing compartments and buckets as needed. These policies will be typically separated into production vs non-production resource access.

Example: Oracle Utilities Customer Cloud Service

The following example references the setup in the Customer Cloud Service (CCS) application outlined above.

File Storage Configuration

- OS-SHARED: This value will point to the Shared Compartment:
  - The user ID will be different in each environment (CCSDEV, CCSTEST, CCSPRODCCS-DEV, CCS-TEST, CCS-PROD)
  - The key ring can be the same in all environment but each environment key ring will have different key pairs (generated separately in each environment).
- Additional values can be defined based on the file location your specific processes will need to access, for example:
  - OS-Payment: for Payment upload interface
  - OS-MR-Up: for Meter Reads upload interface
  - OS-MR-Dl: for Meter Reads download interface
  - The Extendable Lookup values (the name) will be the same in each environment but some of the information that is defined for them will be different in each environment:

* User ID, compartment (Prod vs Non-Prod) and keys.

Recommended Setup for Multiple Cloud Services

If you are using multiple Oracle Utilities Cloud Services (for example Customer Cloud Service and Work and Asset Cloud Service) and you are still using a single Oracle Cloud Infrastructure tenancy (and therefor single Object Storage tenancy), then:

- Duplicate the Cloud Infrastructure setup (compartments, buckets, users, groups, policies, etc), one set with the CCS name prefixed and one set with the WACS name prefix.
- The setup in the Utilities Cloud Service (CCS or WACS) would be identical for both. The differences will be in the references to the various Cloud Infrastructure resources prefixed with CCS or WACS, for example:
  - OS-SHARED in CCS will point to CCS-Shared Compartment with User CCSDEVCCS-DEV/TEST/PROD.
  - OS-SHARED in WACS will point to WACS-Shared Compartment with User WACSDEVWACS-DEV/TEST/PROD.

14

Initial Testing of Object Storage Connectivity

This chapter contains step by step instructions for initial testing of your connection between your cloud service and your object storage. The instructions represent a simple setup for testing the connection to object storage. These instructions do not represent the complete recommended setup that was described in previous chapter.

1. Log into your OCI Console using credentials provided to you by your security administrator:
    a. In the **Identity & Security** menu section, select **Domains** and then select your default domain and from the **Identity Domain** menu, select **Users**:
        i. Create a new user named "INIT-TEST" (Take note of the user OCID).
        ii. Add that user to the Administrator user group.
    b. In the **Identity & Security** menu section, select **Compartments**:
        i. Create a new compartment named "INIT-TEST" (take note of the compartment OCID).
    c. In the **Storage** menu section, select **Buckets**:
        i. Select the INIT-TEST compartment in the **Compartment** field under the **List Scope** section.
        ii. Create the following buckets under the INIT-TEST compartment: CMA- Files
    d. In the **Governance & Administration** menu section, select **Tenancy Details** (under Account Management):
        i. Take note of the tenancy OCID (under **Tenancy Information**)
        ii. Take note of the namespace (**Name** field under **Tenancy Information**)
        iii. Take note of the home region
2. Log into the Utility Cloud Service development environment (DEV), using credentials provided to you by your security administrator:
    a. Go to the **Key Ring** portal (use the Menu Search option):
        i. Add a new Key Ring named "INIT-TEST"
        ii. After creating the new Key Ring, click **Generate Key**.
        iii. In the **Key Pair** section, choose the **Activate** action for the new generated Key Pair.
        iv. Click **View** to get the public key portion of the key pair.
        v. Copy the full content of the public key displayed in a popup window, save it in a text document. You will use this later.
    b. Go to the File Storage Configuration extendable lookup and search for a value of OS-SHARED.
    c. Edit that value and enter the following information:
        i. **User**: The user OCID of INIT-TEST User from step #1.

ii. **Tenancy**: The tenancy OCID from step #1.

iii. **Compartment**: The compartment OCID of INIT-TEST Compartment from step #1.

iv. **Namespace**: The namespace noted in step #1.

v. **Key Ring**: Search for the INIT-TEST key ring created above and select it.

vi. **Region**: The home region noted in step #1.

vii. Click **Save**.

d. Go to the **Master Configuration** portal (use the Menu Search option):

i. Look for the **Migration Assistant Configuration** master configuration.

ii. Make sure that the **Import** and **Export** directories have the following value: "file-storage://OS-SHARED/CMA-Files"

3. Log back into your OCI Console using credentials provided to you by your security administrator:

a. In the **Identity & Security** menu section, select **Users**:

i. Select the INIT-TEST user created earlier.

ii. In the **API Keys** section, click **Add Public Key**.

iii. In the popup window, select the **Paste Key** option and paste the public key value saved in previous step (the public key portion of the key pair generated in the Utilities Cloud Service application), and click **Add**.

4. You are ready to test the object storage connectivity. Log back into the Utility Cloud Service development environment (DEV), using credentials provided to you by your security administrator:

a. Go to the **Migration Request** portal (use the Menu Search option).

b. Search for a Migration Request named Users (F1-Users).

c. Click **Export** for that request (Users).

i. In the popup window enter the file name "init_test" (for example)

ii. Click **Save**. You will be directed to the **Migration Data Set Export** page.

d. Go to the **Batch Job Submission** portal and submit a job with the F1-MGDPR batch code. When the job ends, go back to the **Migration Data Set Export** portal and check the status:

i. If the status changed to Exported, log into the Oracle Cloud Infrastructure Console, navigate to the CMA-Files object storage Bucket under the INIT- TEST Compartment and check that there is a file called init_test.cma there.

ii. If the file exist, the test is successful!

5. If the connectivity test was successful, proceed with the overall setup of the Object Storage and your Cloud Service application per the recommended setup above.

15

Cross-Region Disaster Recovery Considerations

This chapter outlines the considerations for Object Storage connection and configuration in case the cross-regional disaster recovery option has been enabled for your system.

This chapter includes the following:

- Home and Disaster Recovery (DR) Regions
- Preparing your Disaster Recovery Region
- Recovering from a Disaster

Home and Disaster Recovery (DR) Regions

Your system has a Home Region, which is the data region that it was initially provisioned at. This will be referred to as the System Home Region. When cross regional disaster recovery is enabled for your system it will have a designated disaster recovery (DR) region. The disaster recovery region is the data region that your system will be switched to in case your home region is no longer available. This will be referred to as the System Disaster Recovery Region.

Your Oracle Cloud Infrastructure (where your Object Storage resides) also has a home region, that will be referred to as the OCI Home Region. In addition to that, your Object Storage might reside in a different region than your OCI Home Region (Object Storage is a regional service and any cloud account can subscribe to more than one region) the region where your Object Storage will reside and be used for your system will be referred to as Object Storage Home Region.

Home regions examples:

- #1 Typical new account:
  - System Home Region: US-Ashburn
  - OCI Home Region: US-Ashburn
  - Object Storge Home Region: US-Ashburn
- #2 New service to an existing Oracle Cloud Infrastructure account:
  - System Home Region: US-Ashburn
  - OCI Home Region: CA-Toronto
  - Object Storage Home Region: US-Ashburn

If your system has a designed disaster recovery region, it will make sense for your object storage to have a designated disaster recovery region as well, which will be referred to as the Object Storage Disaster Recovery Region.

In most cases the System Home Region will be the same as the Object Storage Home Region but it could be different if it was chosen to be different. The same is true for the System Disaster Recovery Region and the Object Storage Disaster Recovery Region.

Selecting an Object Storage Disaster Recovery Region will be covered in the next section.

> **Note**
>
> If the Object Storage Home Region is different that the System Home Region, you can skip this chapter since the cross region disaster recovery procedures will not affect your object storage and will not affect your system connection to object storage.

Preparing your Disaster Recovery Region

If cross-region disaster recovery was enabled for your system, it will be automatically set up to be ready for a disaster event in terms of availability of resources on your System Disaster Recovery Region, according to your service level agreements.

It is your responsibility to make sure that your object storage is ready as well.

Since Object Storage is a regional service, there is no automatic disaster recovery for that. Assuming your Object Storage Home Region is identical to your System Home Region, you need to plan for the eventuality that this region might become unavailable and so you will need to have your object storage available on another region.

The first thing you will need to do is to subscribe to an additional data region to be your Object Storage Disaster Recovery Region.

In order to subscribe to an additional region you should do the following:

1. In your OCI Console, in the **Governance & Administration** menu section, select **Region Management** (under Account Management) and look at the list of additional available data regions. Select the data region to designate as the Object Storage Disaster Recovery Region (is it recommended to have it identical to your System Disaster Recovery Region, if possible).
2. Your request for subscription to a new data region will be processed and when it is completed, you will see your new region in the list of available regions.
3. You will also be able to switch to this data region in your OCI Console via the **Region** drop-down list.

Copying Your Object Storage Bucket Structure

Your cloud security definitions (for example users, groups, policies and compartments) are all maintained in your OCI Home Region and your identity domains. These definitions are replicated automatically to all the other regions (which you subscribed to) or have their own automatic disaster recovery procedures.

Object Storage Buckets are region dependent which means that each data region can have its own set of buckets.

In order for your system to continue to work properly once it is switched to your System Disaster Recovery Region (for functions that require access to object storage), your object storage bucket structure should exist in your Object Storage Disaster Recovery Region.

Therefore we recommend that you synchronize your bucket structure periodically between your Object Storage Home Region and Object Storage Disaster Recovery Region. This means, at a minimum, that buckets created in your Object Storage Home Region should be also added to your Object Storage Disaster Recovery Region.

Copying Your Object Storage Data

You may also choose to periodically copy the objects inside your buckets from your Object Storage Home Region to your Object Storage Disaster Recovery region.

Please note that copying data from one region to another will result in the use of additional object storage space, which in turn can lead to additional cost per billing period.

Refer to Object Storage Replication in the **Object Storage** section of the Oracle Cloud Infrastructure documentation for more information about configuring data replication policies to copy data between buckets in different regions.

If you have the ability to re-create lost data when a disaster occurs, then you might not need to copy your data across regions in advance, for example:

- Most files generated by your system via batch jobs can be regenerated if necessary
- 3rd party applications that load files into object storage may also be able to reproduce these files upon request

Recovering from a Disaster

A disaster is defined as an event that will cause your System Home Region to become unavailable.

When a disaster occurs, your system will automatically be switched to your System Disaster Recovery Region, based on your service level agreements. When that happens you are responsible to tell the system what object storage region to connect to instead of the current one that is was linked to when the disaster happened (if that region has also became unavailable).

This section covers what you should do during a disaster and after it is resolved.

Switching To Your Disaster Recovery Region

Once your system has been switched to its System Disaster Recovery region, you will need to point it to a different data region for object storage access:

1. Log into each of the system environments.
2. In each environment look at all of your current File Storage Configurations.
3. Edit each File Storage Configuration and change the region field to your Object Storage Disaster Recovery Region.
4. Save your changes.

Switching Back To Your Home Region

When your home region has been recovered and data was restored, the system will be switched back to your System Home Region. At this point you will need to point it back to your Object Storage Home Region for object storage access:

1. Log into each of the system environments.
2. In each environment look at all of your current File Storage Configurations.
3. Edit each File Storage Configuration and change the region field to your Object Storage Home Region.
4. Save your changes.

Copying Back Your Object Storage Data

When you are switched back to your Object Storage Home Region, you may need to copy back some of the data that was created in your Object Storage Disaster Recovery Region. This may also include changes in bucket structure that you may have done while working in your disaster recovery regions.

- Changes in object storage bucket structure can be repeated in your home region manually after that region has been recovered.
- If you need to copy data back to your home region, refer to Object Storage Replication in the **Object Storage** section of the Oracle Cloud Infrastructure documentation for guidance.

Part III
Cloud Monitoring

This section describes how to use Cloud Monitoring with Oracle Utilities cloud services. This includes:

- Status Page

16

Status Page

This chapter provides an overview of the Status Page, which provides the current operational status of the environments and services in your tenancy. This chapter includes:

- Status Page
- Accessing the Status Page
- Subscribing to Status Page Updates
- Events

Status Page

The Status Page shows the current operational status of the environments in your tenancy and informs you of any unplanned and planned maintenance events. An environment's operational status is based on the health checks most recently run on that environment. Health checks are run every few minutes to provide near-real time status updates. The Status Page is unique per tenancy and is only accessible with your Oracle Cloud Infrastructure Identity and Access Management (OCI IAM) credentials. No specific role is required in order to access the Status Page.

Accessing the Status Page

To access the Status Page, users must have a user setup with Oracle Identity and Access Management credentials. No specific roles or environment access is required.

Details for accessing the Status Page for your tenancy can be found in your Welcome email, which contains the Status Page's URL.

If you are unable to find these details, please visit the Oracle Energy and Water Cloud Services - Status Page (Doc ID 2910329.1) knowledge base article on My Oracle Support. This articles contains details and instructions for accessing your tenancy's Status Page.

Subscribing to Status Page Updates

The Status Page is used solely for communicating planned maintenance or unplanned event notifications. Communications for provisioning environments, sizing updates, and so on are not sent via the Status Page.

To subscribe to planned maintenance or unplanned event notifications:

1. Visit the Status Page for your tenancy.
2. Click **Subscribe** to receive notifications.
   You will receive a confirmation email after subscribing. You will not receive notifications about your environments until you confirm your subscription (Please make sure to check your Spam folder).

Events

The Status Page provides information about planned maintenance events. A maintenance event's status is commonly *Scheduled* on a specific date and time, which informs customers of an outage or performance impact ahead of time.

The Status Page also provides information about unplanned outage events. Unplanned outage events inform you of the following:

- **Major Outage** - Main services are down such as Customer Cloud Service
- **Partial Outage** - Supporting services are down such as Customer Cloud Oracle REST Data Services (ORDS)

An unplanned outage event typically transitions through the following statuses:

- **Investigating:** Oracle teams are actively investigating but the reason for the outage is still undetermined.
- **Identified:** Oracle teams have determined the cause of the outage and the resolution.
- **Maintenance**: Oracle teams are performing scheduled maintenance.
- **Monitoring:** Oracle teams applied the resolution and are monitoring the system's operation.
- **Resolved:** The service is back online and operating normally. Oracle teams continue to investigate the cause of the outage, assign corrective actions, and make efforts to prevent the cause of the outage from occurring in the future.

Part IV
GoldenGate Replication

This section describes how to use GoldenGate Replication with Oracle Utilities cloud services. This includes:

- GoldenGate Replication

17

GoldenGate Replication

This chapter provides an overview of the GoldenGate Replication process, which provides a means to replicate data from your cloud service for use in other applications such as reporting, testing, or other custom use cases, as well as specific instructions for administration tasks involved in preparing a target Oracle Cloud Infrastructure (OCI) environment that will receive the replicated data. This chapter includes:

- GoldenGate Replication Overview
- GoldenGate Replication Administration Tasks

GoldenGate Replication Overview

GoldenGate Replication provides the ability to establish one-way, initial, and ongoing change-based (CDC) replication of data from an Oracle Energy and Water Software-as-a- Service (SaaS) cloud service environment (for example, a Customer Cloud Service Production environment) to an OCI hosted Autonomous Database Autonomous Transaction Processing (ATP) target environment (owned and managed by the customer) via a Named Distribution Path.

This provides you with full and direct access to all SaaS data replicated to the target Autonomous Database ATP database instance, and enables you to query, report on, and develop data-driven integrations based on your cloud service data in the target database. It also allows for retention of data that is useful for reporting and integration purposes, even if the data is removed from the source cloud service database via ILM processes such as partition drops.

Refer to Oracle Cloud Infrastructure GoldenGate for more information about Oracle GoldenGate.

Customers must supply the following information to use GoldenGate Replication:

- A source application environment. This is your Oracle Utilities cloud service.
- A Target Tenancy OCID. See Obtaining Tenancy Information for more information.
- A Target Compartment OCID. See Setting Up Compartments and Security Policies for more information.
- A Target VCN OCID. See Setting up Virtual Cloud Networks and Subnetsfor more information.
- A Target Subnet OCID. See Setting up Virtual Cloud Networks and Subnets for more information.

In addition, the customer must also

- Confirm that Identity and Access Management (IAM) policies exist which allow Oracle access to the compartment to create a Private Endpoint (PE).
- Confirm that an Ingress Security Rule to allow Trail Files to enter customer tenancy has been set up. See Setting up Virtual Cloud Networks and Subnets for more information.

- Confirm that the Source environment will not be used for any additional data conversion, factory reset, or clone/data copy (such as where data is copied/ cloned into the Source environment) activities while GoldenGate Replication is active.

Requirements, Prerequisites, and Assumptions

This section outlines specific requirements, prerequisites, and assumptions related to the user of GoldenGate Replication with Oracle Utilities cloud services. Refer to the Oracle Utilities Cloud Services Cloud Service Descriptions document (available from the Oracle Cloud Services Contracts page) for additional details.

Use of GoldenGate Replication requires a subscription to Oracle Utilities Cloud Service, GoldenGate Replication (Part # B110320).

In addition, you must subscribe to the following OCI services:

- OCI Autonomous Database ATP (Autonomous Transaction Processing), which is the target database into which data is replicated.
- OCI GoldenGate Service, which provides the replicate and other GoldenGate services and features for maintaining ongoing replication.

The instructions in this chapter assume customer has:

- An OCI tenancy and administrative privileges in that tenancy.
- Any other users working on OCI components have been created.

The instructions in this chapter assume a fresh compartment. If you are working in an existing compartment, you may be able to skip some of the steps outlined in the GoldenGate Replication Administration Tasks section.

The instructions in this chapter assume the target compartment is in the same region as the SaaS source environment. If this is not the case and data needs to traverse regions, the customer must create a pass through compartment in the SaaS region and connect it to your other region using remote VCN peering via Remote Peering Connection (RPC) on the Dynamic Routing Gateways (DRG) attached to your VCNs. For more information, see Remote VCN Peering using an RPC.

Once all pre-requisite subscription components are in place, your administrators will work with Oracle to establish secure OCI network connectivity between your target OCI tenancy (which is fully owned and managed by you) and the SaaS tenancy in which your Oracle Utilities Enterprise SaaS service is deployed.

The GoldenGate Replication services are designed to support change data capture and replication of regular, Production/Live Operation transactions. To avoid overloading the replication services and/or causing potentially unrecoverable data de-synchronization situations, you may not perform any high-volume data modification activities which are not part of normal, regular Production (live operate) activities in (or into) the source environment while replication services are active. The following actions may only be performed on a GoldenGate Replication source environment once GoldenGate replication services have been disabled, and with the understanding (and acceptance) that these actions will invalidate the ongoing replication and will require full re-establishment of replication services via the source export/ initial load process (which has a usage limit; please refer to the service description):

- Data migration/conversion
- Bulk test data inserts or updates via any provided import tools (such as Content Migration Assistant, or SQL Loader)

> **Note**
>
> Configuration (admin and master data) loads via CMA are not considered bulk data.

- Table truncation
- Factory Reset
- Data copy or clone
- Any other bulk data or destructive environment management operation which would not normally be performed on a production environment during live operation.

Furthermore, performing a data copy or clone into a GoldenGate Replication source environment invalidates the GoldenGate Replication configuration from an infrastructure/ network connectivity standpoint. As this means that Oracle will need to perform re-configuration of the Named Distribution Path, such an activity is deemed a request to "change the Source Environment for a Named Distribution Path" (which has an additional usage limit; please refer to the service description).

Target Environment Sizing Recommendations

The following are minimum sizing recommendations for Target Environments:

- Database – Autonomous Database
  - Single Database
  - Transaction Processing & Mixed (ATP)
  - 4 Peak ECPUs
  - Autoscale ON
  - Database and backup storage as required
- OCI GoldenGate
  - 2-4 OCPUs
  - Autoscale ON

GoldenGate Replication Administration Tasks

This section describes several administration tasks related to use of GoldenGate Replication with Oracle Utilities cloud services. These include:

- Obtaining Tenancy Information
- Setting Up Compartments and Security Policies
- Setting up Virtual Cloud Networks and Subnets

Note that the screen shots in the following instructions may differ slightly from what you see in the OCI Console.

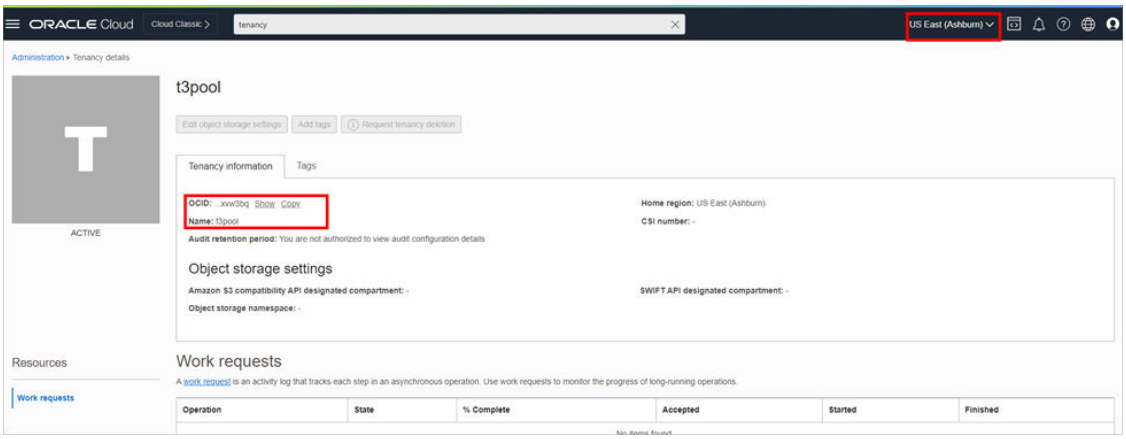
Refer to the Oracle Cloud Infrastructure Documentation for more details about using the OCI Console.

Obtaining Tenancy Information

As noted above, using GoldenGate Replication requires the OCID for the target tenancy. To do this, use the following steps:

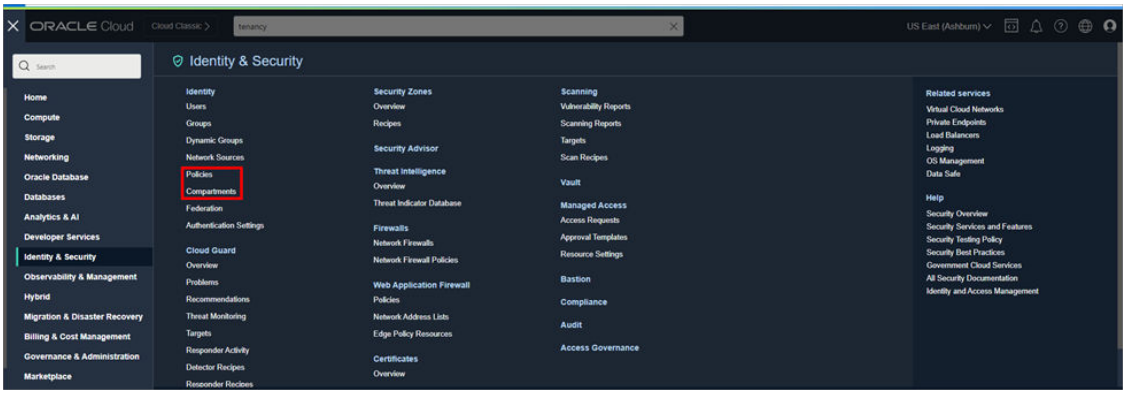
1. Select the **Tenancy Details** option from the **Administration** page.
2. Copy the **Tenancy OCID** and **Name**. This information is required for creating the source and target network path.

> **Note**
>
> If the customer tenancy spans Regions, please ensure you are always in the appropriate region.



Setting Up Compartments and Security Policies

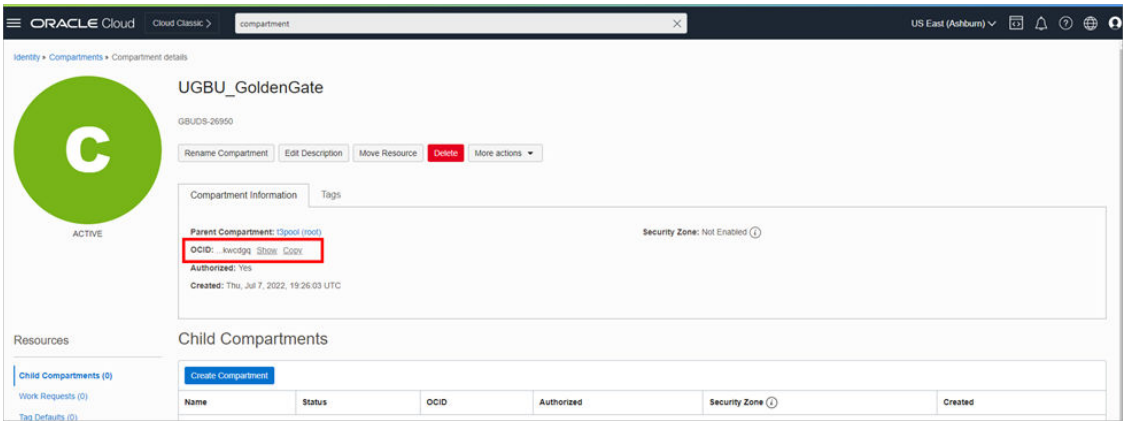
These tasks use the **Compartments** and **Policies** options available from the **Identity & Security** page.



Creating a New Compartment

To create a compartment, use the following steps:

1. Select **Compartments** from the **Identity & Security** page.
2. Click **Create Compartment**.
3. Enter **Compartment Details** for your new compartment:
   - **Name**: Enter a unique name (maximum 100 characters, including letters, numbers, periods, hyphens, and underscores).
   - **Description**: Provide a friendly description.
   - **Parent Compartment**: Choose the compartment where you want to create the new compartment (the root compartment is your tenancy).
   - **Tags** (Optional): Apply free-form or defined tags if you have the necessary permissions.
4. Click **Create Compartment**.
5. Copy and note the Compartment's **OCID**. This information is required for creating the source and target network path.
6. Note the Compartment **Name**. You will need the Compartment Name to build Security Policies.

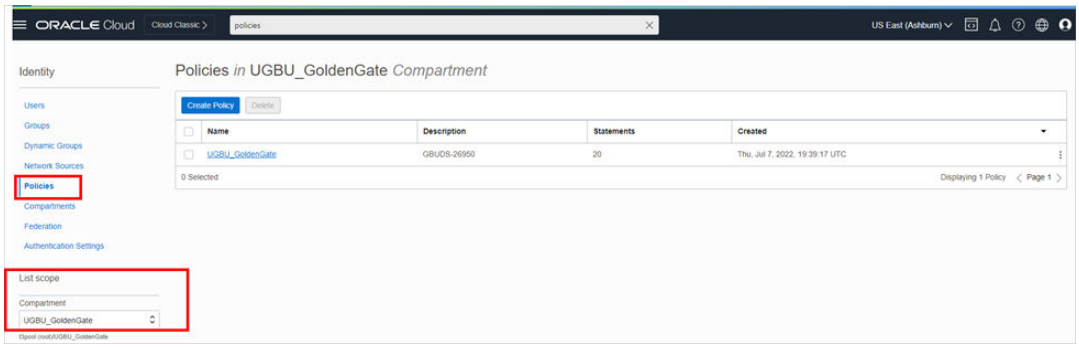


Creating Security Policies

The next step is to create Security Policies that will allow Oracle to create the Private Endpoint in this compartment.

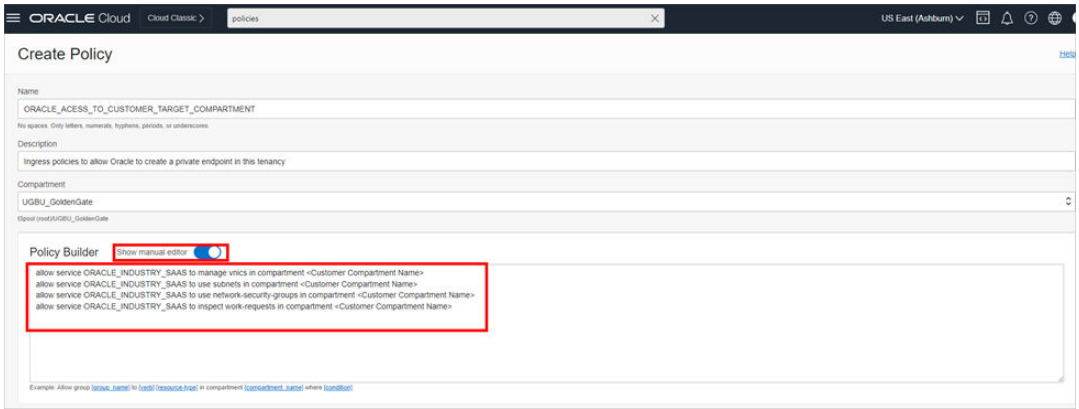
To create security policies, use the following steps:

1. Select **Policies** from the **Identity & Security** page.
2. Click **Create Policy**.



3. Enter details for your Security Policy:
   - **Policy Name**: Provide a descriptive name for the policy. Note that policy names must be unique across compartments.
   - **Description**: Provide a description of the policy's purpose
   - **Compartment**: Select your compartment from the **Compartment** drop-down list.
   - **Policy Statements**: The Policy Builder wizard does not support all types of valid policies, so you must use ‘Show Manual Editor to create the policy statements needed for GoldenGate Replication.
   - In the **Policy Builder** box, manually create the following policy statements:
     - `allow service ORACLE_INDUSTRY_SAAS to manage vnics in compartment <Customer Compartment Name>`
     - `allow service ORACLE_INDUSTRY_SAAS to use subnets in compartment <Customer Compartment Name>`
     - `allow service ORACLE_INDUSTRY_SAAS to use network-security- groups in compartment <Customer Compartment Name>`
     - `allow service ORACLE_INDUSTRY_SAAS to inspect work-requests in compartment <Customer Compartment Name>`

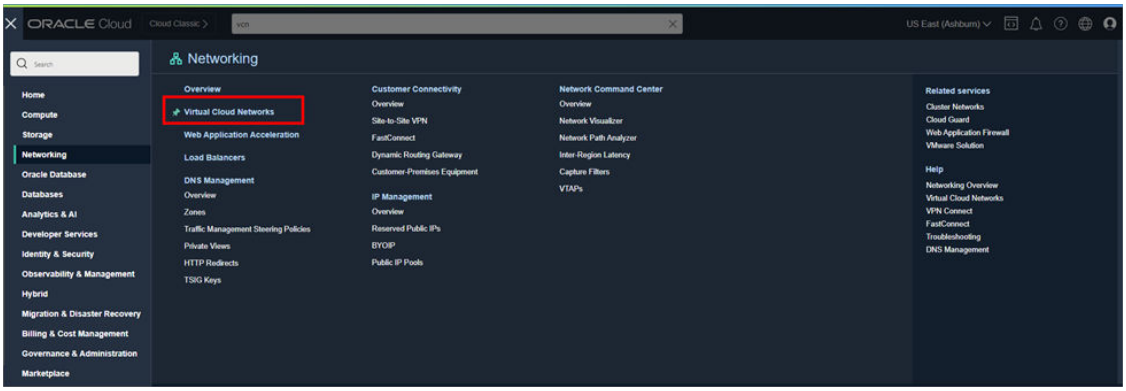
     where `<Customer Compartment Name>` is the name of the compartment you created earlier.



4. Click **Create** to create your security policy.

Setting up Virtual Cloud Networks and Subnets

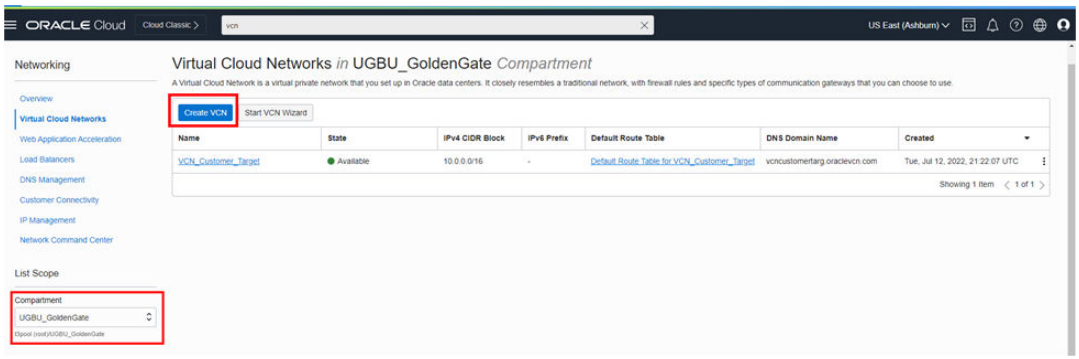
These tasks use the **Virtual Cloud Networks** option available from the **Networking** page.



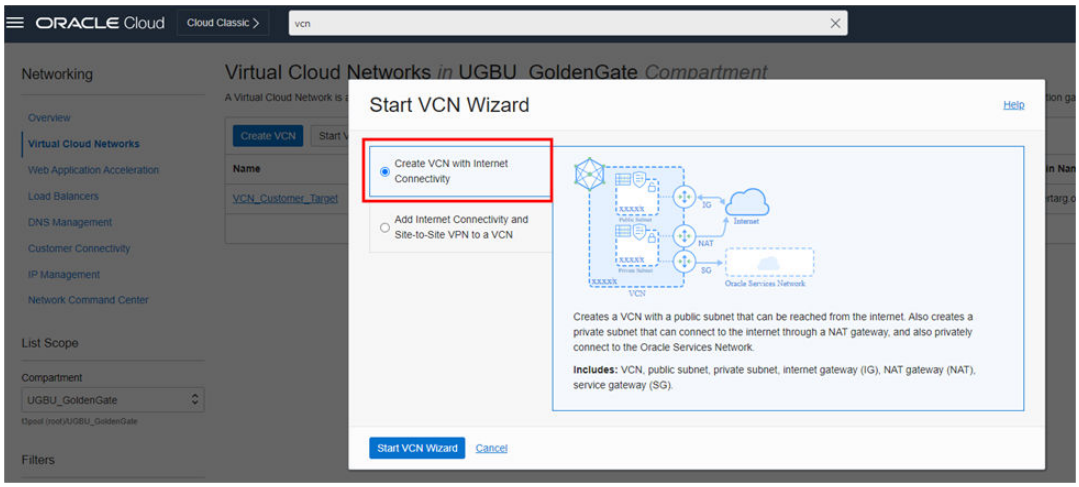
Creating a Virtual Cloud Network

To create a virtual cloud network (VCN), use the following steps:

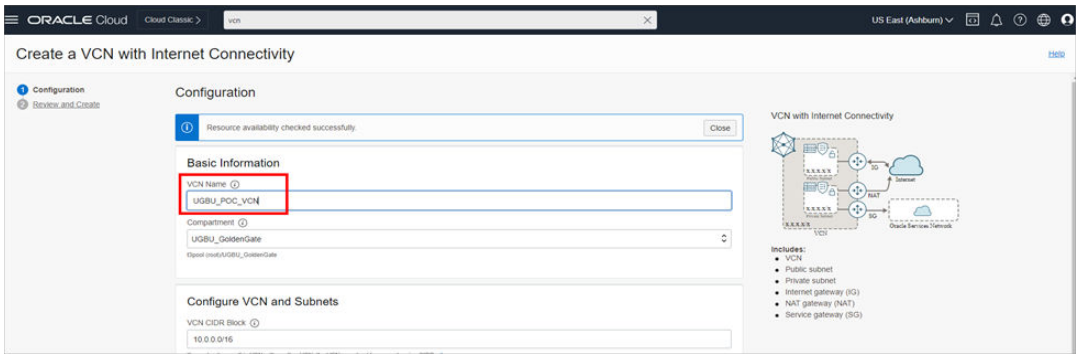
1. Select **Virtual Cloud Networks** from the **Networking** page.
2. Select your compartment from the **Compartment** drop-down list.



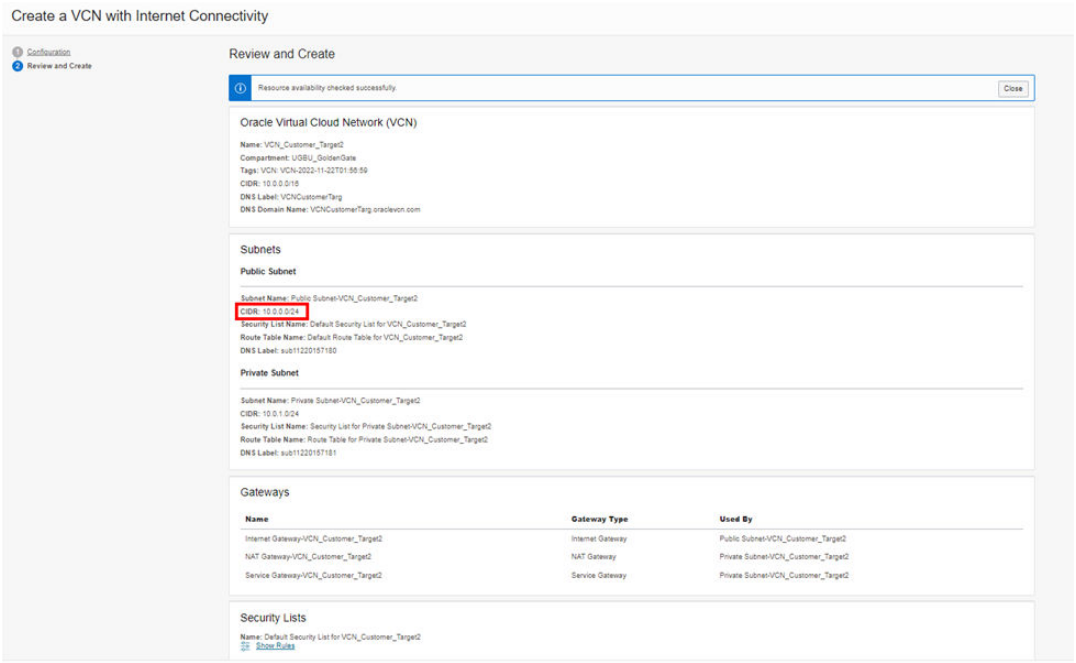
3. Click **Create VCN** to create a new virtual cloud network using the **VCN Wizard** (make sure that you are working in the appropriate compartment). The **Start VCN Wizard** panel opens.
4. Select the **Create VCN with Internet Connectivity** option. Note – Replication out of SaaS does not require all of the resources created by the VCN wizard. However, this is the simplest way to create the VCN and subnet required for replication out of your cloud service and will provide other networking resources that may support the use cases for accessing data.



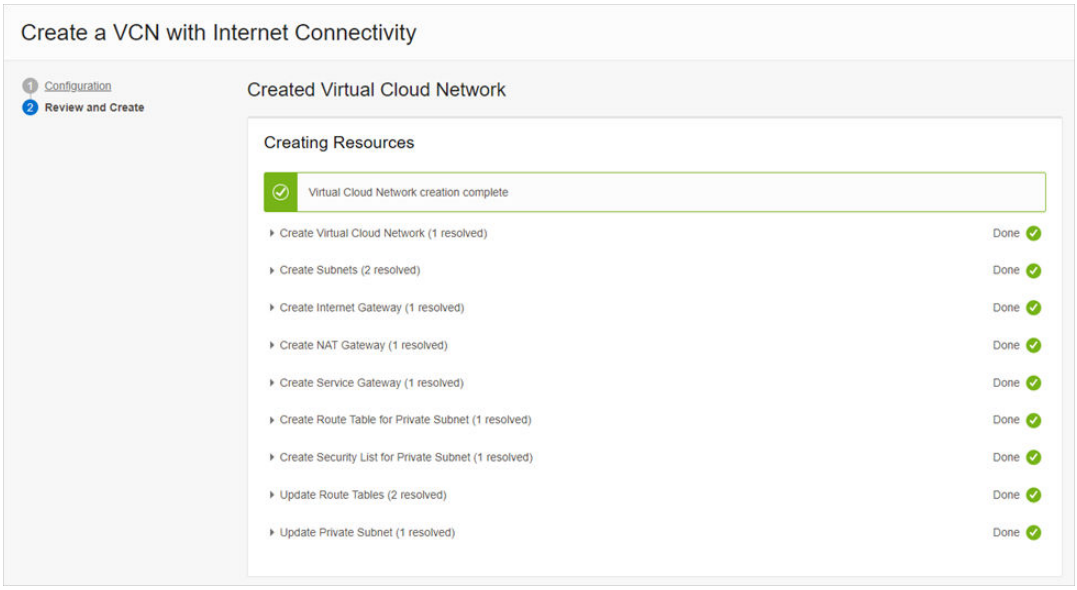
5. Enter a **VCN Name**. Accept all other defaults and press **Next**.



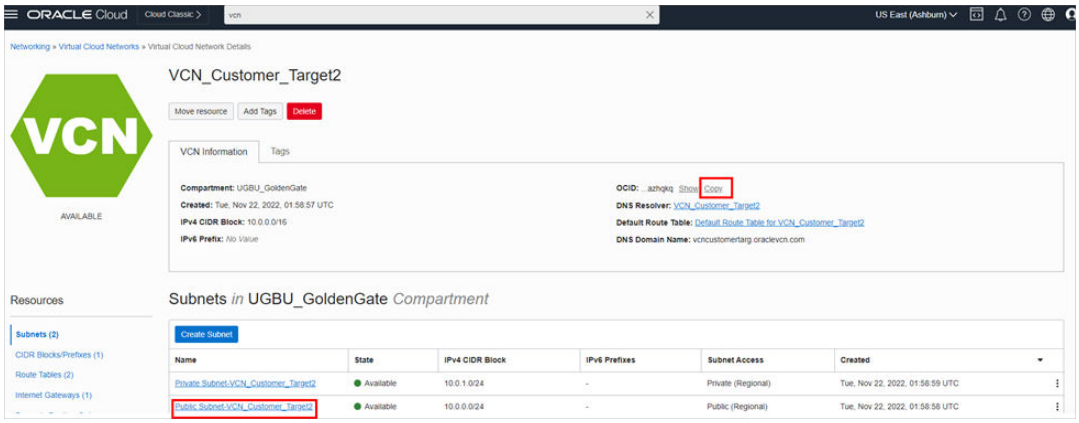
6. Review the virtual cloud network resources and note the **CIDR** for the subnet (in the **Public Subnet** box). Your Target environment resources will be associated with this subnet.



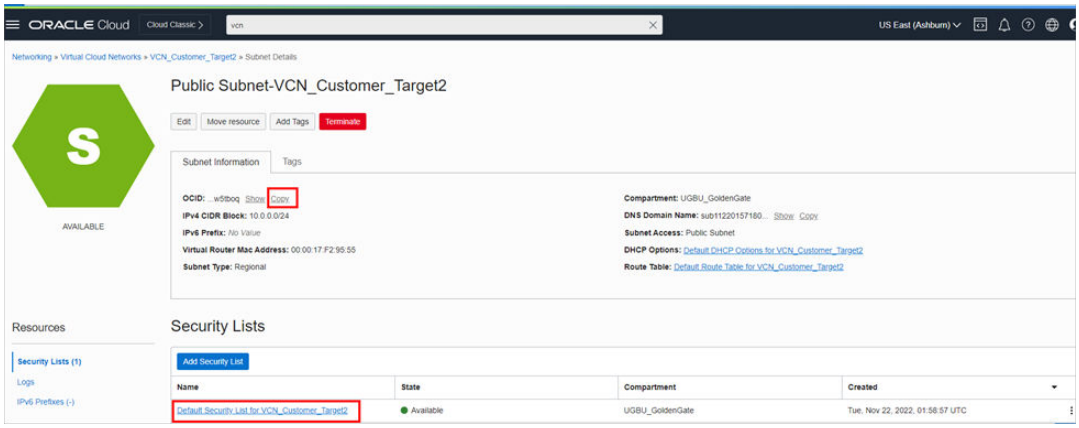
7. As the resources are built for the virtual cloud network, the **Created Virtual Cloud Network** screen will display a list of resources and statuses.



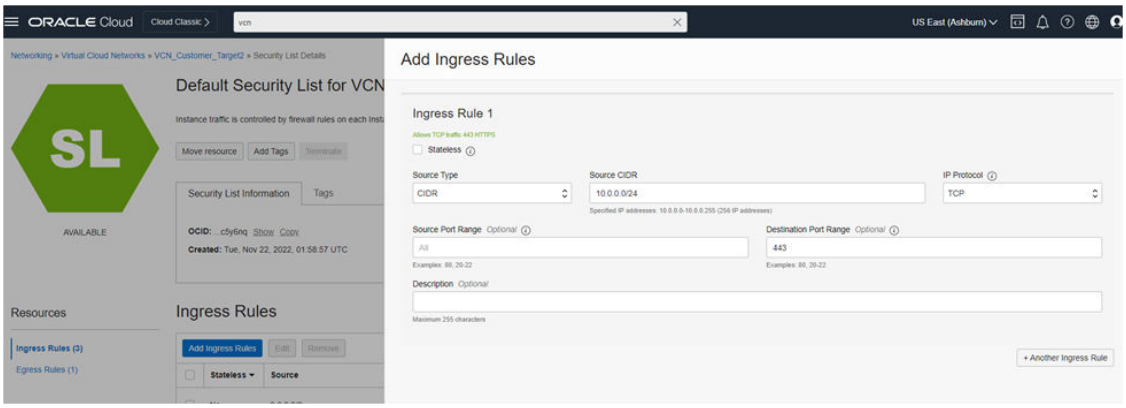
8. Close the **VCN Wizard** to view the Virtual Cloud Network. Copy and note the VCN's **OCID** and **Name**. This information is required for the Network Path Creation.
9. Click the **Name** of the subnet where you would like your Target environment resources to be located.



10. Copy and note the Subnet's **OCID**, **Name**, and **IPv4 CIDR Block**. This information is required for the Network Path Creation.
11. Click the **Default Security list** associated with this subnet.



12. Click **Add Ingress Rules** to add an Ingress Rule to the default Security list. This Security Rule is prerequisite of the Environment Creation.
13. Configure the Ingress Rule as follows:
    - **Stateless**: Leave this checkbox unchecked to make the rule stateful (this means that any response to the incoming traffic is allowed back to the originating host, regardless of any egress rules applicable to the instance_.
    - **Source Type**: Select "CIDR".
    - **Source CIDR**: Enter the subnet's **IPv4 CIDR Block**.
    - **IP Protocol**: Select "TCP".
    - **Source Port Range**: Leave blank
    - **Destination Port Range**: Enter "443".
    - **Description** (Optional): Add a descriptive string for the ingress rule.



When the above steps have been completed, the required resources, policies and security rules will be in place to support GoldenGate Replication.

Note that this document shows only the OCI components required to implement the basic Replication out of Oracle Utilities SaaS. It is likely that your production OCI architecture will contain additional components as required by your production requirement.

Glossary

Index